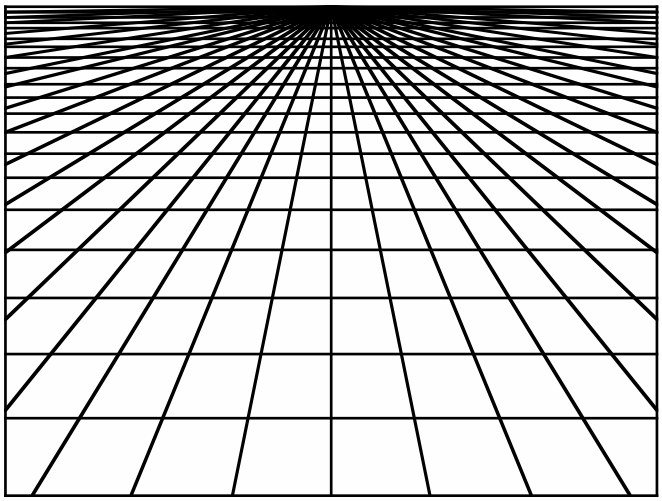
UNIVERSITY OF OSLO
FACULTY OF SOCIAL SCIENCES

TIK
Centre for technology,
innovation and culture
P.O. BOX 1108 Blindern
N-0317 OSLO
Norway
http://www.tik.uio.no

Universiteit Maastricht



ESST
The European Inter-University
Association on Society, Science and Technology
http://www.esst.uio.no

The ESST MA

Privacy and Functionality in an Ambient Intelligence Application

Lars Ødegaard
University of Oslo / Universiteit Maastricht
Technological Culture
2006

Word count: 21680

Name: Lars Ødegaard
E-mail: larsoe@gmail.com
1st/2nd semester universities: University of Oslo / University of Maastricht
Student number University of Maastricht: 0393428
Specialisation: Technological Culture
Supervisor: Jessica Mesman
Word count: 21680

Synopsis: Computerised, networked systems are diverging, creating a society where humans are constantly connected to various systems, creating electronic traces of their actions throughout the day. Modern computers enable these traces to be gathered from various sources and analysed. This can create better functionality for the humans but the cost might be their privacy. This thesis will examine the ambient intelligence concept through a case study of the SensorPhone, a system designed to gather information on the users movement and encourage a healthier lifestyle. Gathering and sharing information is necessary for the system, but might simultaneously pose privacy challenges.

***Keywords**:* Privacy, Functionality, Ambient Intelligence, Perception, Treatment

Preface: This thesis is the final result of the ESST masters program at the University of Oslo and Maastricht University.

I would first like to thank Jessica Mesman, not only for agreeing to supervise me on this thesis, but also for her lectures at the university. Her input and directions have been invaluable. Frank Vlaskamp and Thijs Soede, at the Institute for Rehabilitation Research have helped me greatly and provided insight into the topics of ambient intelligence and health-care. They have also been kind enough to provide me with an office for a major part of the writing. I would also like to thank Robert Childs at Vodafone for giving me the opportunity to work with the SensorPhone program and providing me with people to interview.

I have found it interesting and stimulating to work with the SensorPhone case and will certainly try to follow the development of the project in the coming. I firmly believe that the potential for the system is tremendous and that it can help both in the treatment of different conditions and relieve the pressure on the health-care systems where it is put into practice.

Privacy, which is the main topic throughout the thesis, is something I think should be valued, and I think society needs a discussion on privacy issues. Privacy is challenged from technical devices, Internet, corporations and government, and one can wonder how the “little man” can preserve his freedom when facing such strong actors.

I would also like to take the opportunity to thank my family and friends, and of course the ever so lovely Emma, for their patience and support in the months of the writing.

1. Introduction

Ambient intelligence is considered by some to be the "next big step" in technology. The technology can be used to improve life as we know it and solve many of the problems that society face. A world where one can communicate with anyone and anything, anytime and anywhere seems attractive to many. However it is most difficult to assess that from our knowledge at the present time. The technology is in the making and exists primarily on the drawing board and as visions of researchers and industrialists. Some of the components that ambient intelligence (AmI) relies upon exist today while others still have to be developed.

A brief description of AmI will be a divergence of ubiquitous computing and a human centred interface. Miniaturised computers embedded in everyday objects with the aim of aiding humans with what they want or need at the appropriate time (Brey, 2005).

AmI is predicted to be not only the result of technological progress but also a shift in how humans interact with each other and the environment. The utopian view is a future where technology aids humans in all aspects of everyday life and promotes human interaction. While the dystopians think of an AmI world as a place where machines override humans in their decision-making and alienates them in their own world[1]. What is clear is that the technology, if introduced, will greatly affect humans and how they interact with technology and each other.

To ensure that AmI will become a technology that the public will accept and embrace, a number of issues have to be dealt with at an early stage. The ISTAG group[2] calls for a discussion on how society wants a number of issues to be handled. These issues range from protection of personal identity, protection against intrusion by both public and private actors, protection of the individual sphere, protection

against discrimination, access to information, free speech, trust and so on. Social, economic, legal and technological aspects should also be taken into account in this debate (Friedewald et al., 2005)

The issue within AmI that I found most interesting, and that I claim is a most important issue within a democratic society, is that of privacy. Privacy is directly linked with functionality in AmI devices and services due to a requirement for proper identification. Identification of the user on some level is required to customise services and arrange payment. Information about users and the utilisation of services are collected, stored and employed to create profiles in the learning computer systems. This again can create increased functionality for the user, with customised and more relevant services, but the cost might be anonymity and privacy.

Designers of AmI devices have to address these problems during the building of the systems. Their values, morals and priorities regarding privacy issues and functionality will be inscribed into the system as it is being built.

This leads me to my research question:

How will the designers of technology inscribe privacy and functionality interaction in an ambient intelligence device?

The interest in this for our technological culture is that privacy is increasingly challenged by functionality. Electronic devices and computerised databases are increasingly gathering information, and services are created as a result of this information. AmI will be entirely dependent on information gathering and intelligent

processing of it. Therefore it is most important to create a discussion on how one can increase functionality without undermining the democratic necessity that is privacy.

1.1. The Methodology

To be able to explore and explain this question I will use one of Vodafone Netherlands research projects as a case study. They have been kind enough to give me access to their data and personnel. The SensorPhone, as the project is named, is not entirely an AmI system but it does fulfil some of the criteria in an AmI. The SensorPhone's relevance to AmI will be discussed in the last part of chapter three.

This research program is interesting because it is, or rather is intended to become, a health application. There are hopes within the research community that AmI will have a significant impact on health and treatment. In the case of the SensorPhone's the first focus will be in the treatment of obesities and later on a wider range of diseases. I have chosen to view AmI and then the SensorPhone as an extension of telemedicine. Gringsby and Sanders (1998) view telemedicine as treatment when the doctor and patient are separated by time and/or space, using telecommunication channels as methods of communication. The SensorPhone represents a new way of viewing treatment. With ambient technologies, a doctor can follow his or her patients much closer, diagnosis can be determined with data gathered over time and the progress of the treatment can be constantly evaluated.

An interesting aspect of the discussion surrounding AmI is that the topics discussed are similar to the discussion on the European Union's plans for electronic healthcare records for all its citizens. The introduction of such records faces similar problems when it comes to identification, authentication, ownership of data and privacy issues (NICTIZ, 2006). The data that the SensorPhone creates will most likely

become a part of theses healthcare records, thus having to follow the same regulations to become a “trusted party.”

To be able to perform an analysis I will rely on literature research and interviews conducted at Vodafone as my empirical data. The literature on privacy and ambient intelligence is taken from sources that are either doing research on the subjects or governmental organisations that oversee privacy laws. The interviews were conducted amongst selected employees at Vodafone. Two of the interviewees were from the research and development department, both of these had previous knowledge of the SensorPhone. The three other employees held positions in the operational sections of Vodafone. Their positions were in the marketing IT-security and the legal department. None of these three had any relations to the SensorPhone project, but they represent company functions that will affect a final product. The last three interviews were based on an open structure as opposed to a list of preset questions. The interview was divided into two segments where the first half was on general privacy risk in the interviewees’ daily job. In the second half the interviewee were presented with the SensorPhone and questioned on how they viewed it in the light of a risk to privacy. Since the project is only at a research stage I found it most relevant to look at sources within Vodafone. This provided me with insight in to what the organisation may wish a new product to do.

My tools of analysis in the relationship between the technology and user will be Adams and Sasses (2001) model of privacy in a multimedia context. The model was originally developed for situations where video and audio data were recorded and shared, such as in video conferencing systems. In addition it has shown to be suitable in several other situations where users expose themselves to technology, the model gauges their reaction.

Theories and concepts from actor-network theory will be used to look at the technology from the producer's point of view. Akrich (1992) claims that the anticipation that the builders have towards the potential users will be inscribed into the objects they design. Therefore I have sampled their views of the potential user when analysing the SensorPhone with Adams and Sasses model. I have integrated the voice of the interviewees into the text, not separating their statements distinctly from the rest of the text. This is due to lengthy statements and discussions with the interviewees. However I believe that I have managed to maintain the interviewees' original thoughts and meanings. I will, in this analysis limit myself to the segments of obesity and fitness.

Vodafone is not the only organisation that has helped me with this thesis. The Dutch Kenniscentrum voor Revalidatie en Handicap, or The Institute for Rehabilitation Research (iRv) have been enough kind to aid me with their expertise on rehabilitation. The institute aims to improve life for the disabled through applied research. The iRv does contract research for Vodafone on the SensorPhone project to ensure that the medical part of the SensorPhone is satisfactory.

1.1.1. The Structure of the Thesis

The structure of this paper is divided into five main chapters. In addition there is a synopsis in the start of the document, an introduction and a bibliography.

The first chapter is this introduction that presents the research question and the topic briefly.

The second chapter is a review of the concepts of the thesis. It begins with a discussion on ambient intelligence, and then continues by presenting some aspects of telemedicine and the future of health care. The concept of privacy is also outlined, it's

definition and why it is increasingly more difficult to maintain it and at the same time more important to maintain it.

The case of the SensorPhone, with its different components is described in chapter three. The description includes the problems the SensorPhone is planning to solve, and its relation to AmI. The chapter will also describe three different segments of users that Vodafone inscribes into the system. Two of these segments will be within the first stage of development while the last segment is more of a vision in which way the technology should develop. Further, the chapter describes how the SensorPhone is a step on the road towards an AmI world and some of the threats in the system.

In chapter four a model of how the user of technology views privacy is presented and the SensorPhone is analysed within the components of the model. Three scenarios that illustrate how functionality and privacy are connected are also presented. The last part of the chapter suggests a strategy for how to survey the SensorPhone test group in the aspect of privacy.

Chapter five will an analysis based on the interviews from Vodafone and their thoughts regarding the SensorPhone. How the employees view such a system, which risks they immediately associate with the system and their thoughts regarding a solution to the risks. I will also explain a few forces that affect the development of the system and how may affect the system. There will also be a discussion on how internal and external processes function as guardians of morality in the system.

The final part of the thesis is a brief summary, where some implications for Vodafone are outlined. There are also a few suggestions for further research that suits the science and technology studies. The Appendix briefly describes ISTAGS ambient intelligence scenarios. Notes can be found at the end of each chapter.

[1] For utopian scenarios read Ducatel et al. 2001, for the dystopian scenarios see Punie et al. 2005.

[2] Information Society Technology Advisory Group (ISTAG) is funded by the European Unions Sixth Framework Program to research Ambient Intelligence

2. Visions of Ambient Intelligence

In this chapter I will briefly explain how Ambient Intelligence (AmI) is envisioned to affect our society and some of the challenges that it poses. I will discuss some of the concepts relevant for my research question and the view of the industry, scholars and advocates within the fields of AmI, telemedicine and privacy.

I have chosen to focus on the development and research of AmI in Europe, even though research is extensive both in the United States and Japan (Friedewald et al., 2005).

It is important that the reader keeps in mind that AmI is not just one technology, it is a concept with the potential to change how people interact, both with each other and with objects in their surroundings. AmI will not suddenly be invented and appear in our life; it will consist of a multitude of technologies that converge gradually and for the full implementation major socio-economic changes will be required (Ducatel, 2001, p. 14).

I will explore the debate surrounding AmI and its uses, especially within the field of medicine. AmI can be viewed as an extension of the telemedicine concept if we acknowledge Gringsby & Sander's (1999) definition in which telemedicine covers all aspects of health-care where services can be transmitted over a distance using telecommunication technologies.

One of the greatest challenges in AmI is the way in which privacy issues should be dealt with. A system that has the purpose of gathering, processing and sharing information about its users continuously, creates privacy challenges that should be discussed early in the process of building the technology.

2.1. Ambient Intelligence

Emile Aarts, vice president of R&D in the Philips Company coined the term Ambient Intelligence (AmI) in 1993. The term describes a concept where networked computers are acting as personal advisors. This concept is vaguely defined as a system where the three technologies of ubiquitous computing, user interface design and ubiquitous communication all converge (Friedewald et al., 2005).

Ambient intelligence is considered to be the "next step" in computing, where the users move away from stationary machines towards a networked system that is part worn on the body, part carried like a mobile telephone and part embedded in our surroundings (Ducatel, 2001). Computers will disappear as distinct objects (Brey, 2005). The emphasis is on greater user-friendliness, more efficient service support, higher user-empowerment, and more support for human interactions than on current computers (Ducatel, 2001).

The main idea of AmI is that *everything* has sensors and some computing power embedded, and that these sensors can communicate the status of the object it is attached to. One object can then communicate with another and with humans through Personal Information Managers (PIM), a technical device, or through different interfaces[3]. An example of this communication is a refrigerator that asks the milk bottle inside about how much milk is left and its expiration date, before it creates and transmits a shopping list to its owner's PIM or, if the user has allowed it, directly to a grocery store for home delivery. In a more social setting one can imagine AmI handling a taxi queue, lets say at peak hours when there are more people travelling than the number of taxis. AmI can sort the queue based on who goes where and put several parties in the same taxi, thus creating travel plans for the taxis. This could benefit society in several ways; congestion due to traffic would decrease, the traveller

could pay less due to taxi sharing and the average waiting time in the queue would decrease.

These examples are just to illustrate the potential dataflow in AmI, the goal is much wider than that. Computing and networking should be ever-present. Ranging from a sock that analyses itself and then tells the owner that it needs a wash, and how it should be washed, to systems that assess a major road accident and automatically communicated with emergency services in addition then they re-route other traffic from that road. Objects with embedded computers should be able to communicate wirelessly with the relevant object to fulfil the AmI potential (Brey, 2005).

There is no commonly agreed on definition of AmI yet, but Casert (2004, p. 4) states that it is about technology knowing where *you* are and what *you* need. Further he states that the current state of AmI is a Hollywood version of everyday life (2004, p. 4). Most effort is spent on spectacular or glamorous sectors of life and not enough on the useful but humdrum.

In the term Ambient Intelligence, the word *ambient* refers to something that is in the immediate surroundings. While by *intelligence* one usually assumes that some ability to use knowledge should be present. In AmI this is not the case, so far it is not envisioned that real intelligence is present, users will only assume that it is intelligent since the reason for an action is based on information and statistics that the user does not always recognise.

Emiliani and Stephanidis (2005, p. 606) regards that AmI as a concept is under development and that it is not yet clear what it will evolve into. However, they consider it likely to follow the trends in the emerging information society. According to Emiliani and Stephanidis (ibid.) some of these trends include:

- Communication through a multitude of channels.

- Communication through user representatives (automated agents and avatars)
- Presenting information in multiple media types.
- Multimodal interaction, through sensors and motor abilities.

The Information Society Technology Advisory Group (ISTAG) has done extensive research on the field of AmI as a part of the European Unions Sixth Framework Programme. Much of their work has been to create scenarios to describe plausible futures. ISTAG do not view this as predictions on the technical development but rather a tool to create discussions on AmI and its implication (economic, social and political). Their hope is that a discussion will lead to an improved vision and collective understanding of AmI and its potential impact (Ducatel, 2001). ISTAG's first four scenarios are created to examine the potential of AmI along two axes, the individual to community and the efficiency to social humanistic (ibid.). In addition they developed four unwanted scenarios to identify risks, challenges and barriers in an AmI world (Punie et al., 2005). The scenarios are not clearly distinct from each other, but rather complimentary (Ducatel, 2001). A brief description of these scenarios is presented in appendix A in this paper.

The common ground in the four scenarios is a human centred interface. This emphasises ISTAG's view that AmI development should be focused on the needs and cognition of humans, not driven by technological possibilities (Ducatel, 2001).

ISTAG's assumptions are that the scenarios in the *individual* categories will be achieved earliest. The individual scenarios do not require the major changes in the infrastructure, public behaviour and the socio-economic situation that the community

scenarios demand. Rather it focuses on incremental changes and interconnection in today's technology.

To describe the uses of AmI is difficult, not only because it is in an early stage of development, but also due to the extent it can affect our society and the number of paths it might follow. If the AmI saturation in society is ever complete it will affect the individual 24 hours a day.

2.1.1. The First Use of AmI

Most of the publicity that AmI receives, both from scientific and popular sources, is in the domain of *Smart Home*, *Intelligent Home* and *Automated Housing.* There are already objects in some houses that can be viewed as a step towards AmI, devices such as digital video recorders (e.g. www.tivo.com) and energy management systems. The Tivo video recorder is a new step in how we view TV according to their website. The system can automatically connect to an electronic TV-guide and record the users favourite shows throughout the season, regardless of the user presence, channel and time. This is a step forward from traditional video recording where the user had to explicitly specify when each recording should start and stop. The Tivo system relieves the user from this tedious, manual task and enables the user to view favourite shows when it is suitable.

Ducatel (2001) argues that the lead market when different systems truly start to interact will be in the business sector. This is explained with the argument that efficiency requirements in the business market which outrank price sensitivity. This is similar to previous situations where the business sector has been an early adopters of technology, such as the personal computer and mobile telephones.

A third view is that AmI development will start in the health sector. AmI can contribute in a number of ways in the diagnosing and treatment of diseases in addition

it may promote independent living for the elderly and those with disabilities (Celler et al., 1999; Casert et al., 2004). This will represent major changes in how we view health-care and treatment.

2.2. A New Perspective on Health Care and Treatment

Telemedicine, telecare and eHealth are three concepts with one common ground: The doctor can treat the patient without actually being in the same room. The traditional and most used way of applying telemedicine has been to provide specialist consultancy to small rural hospitals or other remote locations[4] through a video link, instead of the consultant travelling there. Other uses include sending laboratory results, medical records and diagnostic images for analysis through electronic telecommunication channels (Gringsby and Sanders, 1998) as opposed to the slower postal or courier services.

Although telemedicine has been around since the 1960's its use is not widely used. A 1996 survey among 2400 non-federal rural hospitals in the USA showed that only 17% participated in telemedicine networks, and that an estimated 21 000 patients were consulted that year (Gringsby & Sanders, 1998). Some of the reasons for the low number of participants in telemedicine networks are quoted to be high cost of equipping interactive video, lack of reimbursement, unclear regulations regarding malpractice and liability issues and concerns about the security of electronic medical data and records.

If we are to believe the predictions and estimates of AmI advocates the number of participants in telemedicine will rise tremendously in the future. Researchers and policymakers will find solutions for the problems quoted by Gringsby and Sanders, and the cost will decrease as the technical development progresses.

AmI can be used to prolong the time elderly live outside care-centres and provide inclusive technologies for those with disabilities (Casert et al., 2004). It can dispatch emergency workers to an accident site and provide medical data from the injured (Punie et al., 2005). Also there is the possibility to gather medical data from patient with chronic diseases and advise if changes in their condition (Celler et al., 1999). These are just a few examples of how AmI might change the field of medicine. Underlining these changes we can see a paradigm shift in how doctors work, how patients communicate with physicians and how treatment occurs.

The traditional concept of treatment is where a patient contacts the physician with a specific problem; the doctor examines and provides a method of treating the symptom. The alternative to this is that the doctor discovers a problem during a periodical exam and provides treatment to cure the patient. In the AmI setting, the doctor and patient can be separated both by place and time.

When an individual in an AmI environment uses a Personal Information Manager (PIM) fitted with health monitoring sensors it enables a range of possibilities. Consider a patient in either a high-risk heart disease group or a patient that suffers from mild dementia. If these patients are fitted with a health monitor connected wirelessly to a doctor's office, then the doctor will be able to detect changes in heart rhythm or in behaviour and can take the necessary precautions (Celler, 1999). The detection here can be a result of both manual revision of a patient's data by the physician or automated software agents that "flag" a patient when a preset limit is breached.

In situations where patients are fitted with a PIM and medical monitors either for diagnostic purposes or as part of a treatment, the physician will be able to trust the information to a higher degree. Also the information will be gathered over time, thus

creating a better picture of the condition than a sample of data collected in the doctor's office. Medical data, such as heart rate and blood pressure can be monitored over time, not just sampled during an examination. Movement and medical data can be tracked and show whether or not the patient is following recommendations from the physician. Thus, eliminating the uncertainty on whether or not the patient is truthful when asked about exercising or other factors.

For many of us AmI will tell the tale of a more efficient and comfortable tomorrow, while for the disabled, AmI can be the difference between dependency and autonomous living. AmI can decrease the need for human care support and promote secure and safe living. Further, AmI can motivate and stimulate people within the scope of their abilities (Soede, 2005).

There is also a financial gain from fitting patients with AmI, either for diagnostic purposes, for treatment or even as an assisted living application. The patients will be able to stay in their own home to a higher degree, thus saving hospital space, bedtime and money directly affecting the health budget. There will also be a larger socio-economical benefit since a patient in some cases will be able to continue working instead of staying at the hospital or visiting the doctor.

2.2.1. Criticism in AmI Related to Health Care

A concept that changes the way we think about health care will also include negative elements. Some factors perceived as positive for some groups, will be viewed as negative for others. Celler et al. (1999) reports that in Britain, 15% of all home-care visits by a nurse could be replaced by telecare. At the same time studies in the US concluded that 46% of all on-site nursing activities could be replaced by telenursing. While this is indeed positive news for a strained health budget, it may not be so for the users of nursing services. I assume here that for many of these users the human

contact of a nurse visiting may be as beneficial as the medical care that the nurse provides, as loneliness is a problem for many elderly and disabled.

Einar Aas extends the argument that technology cannot replace personal care (Casert, 2004). His claims were that what is lacking from care-homes is enough care. The technology that can change this is in place, but is not yet integrated into a social setting.

Aas also recognised privacy in AmI applications in the care-homes (Casert, 2004). How can the user be assured that medical records are well protected? His question is one of the more fundamental in AmI research. How security and protection of the users personal data and privacy should be dealt with is one of the major obstacles that have to be addressed before AmI becomes a reality. Soede (2005) states that privacy is a major concern in the treatment of chronic illness or the disabled, while in the critical care all focus is on life saving.

2.3. Privacy

Why do people need privacy? I have searched for a good, simple answer for this, but can only conclude that such an answer does not exist. As with free speech, privacy is an important part of democracy and one of the corner stones in modern society. The protection of privacy is outlined in Article 8 of the European Convention on Human Rights. The United States constitution protects privacy although not mentioning it explicitly. Privacy is also protected in the UN charter. Evidently the democratic countries in this world have laws that protect the privacy of its citizens (Blarkom et al., 2003).

One of the most quoted definitions on privacy is by the philosopher Westin (1967) *"the claim of individuals ... to determine for themselves when, how and to what extent information is communicated to others."*

The Handbook of Privacy and Privacy enhancing technologies (PISA) provides two characteristics of privacy in the information age (Blarkom et al., 2003):

- The right to be left alone.
- The right to decide oneself what to reveal about yourself.

A person goes through different roles in life, and switches between those roles several times a day. Privacy can be tied to a wish to separate private, public and professional roles.

As early as in 1890 two judges published a landmark article in the Harvard Law Review, calling out for privacy laws in USA as a response to the development of newspapers and photography. They claimed that *"numerous mechanical devices threaten to make good of the prediction that what is whispered in the closet shall be proclaimed from the house-tops."* And "*gossip ... has become a trade"* (Warren and Brandeis, 1890, p. 2). Warren and Brandeis saw that in an advancing civilization, man would find solitude and privacy more and more essential to the individual. The complex and intense society had the ability to spread apparently harmless gossip that when persistently circulated has the potent of evil.

Even though Warren and Brandeis published this in 1890, their concerns are no less relevant today. The traces left electronically by individuals today are gathered by numerous organisations, and the usage of these data is often not clear to the individual.

It is agreed on that information given voluntarily from an individual to an organisation for a specific purpose can be used in the way intended. However, when information gathered for one purpose is used in a way that was not disclosed to whom the information was gathered from we see a breach of the trust vested in the gatherer. Such 2nd level usage of data will be discussed further in the next chapter.

2.3.1. The Publics Awareness of Privacy Issues

How much individuals know and care about their privacy is debatable. There seem to be consent that the advantages of privacy loss often outweigh the disadvantages. This can be seen in the discussion on surveillance cameras as a tool to prevent crime. The general public's acceptance of cameras in public places is increasing (NDPA, 2006).

If we look towards the government position, most European countries have a system for protecting privacy, through laws, sanctions and regulatory bodies. However, laws and regulators are under constant pressure due to public demands for security against crime and terror. The priority is most often short-term security before long-term privacy protection.

According to the Eurobarometer (European Commission 2003) 60% of all EU citizens were concerned to a greater or lesser degree about the issue of personal privacy protection. The British Information Commissioners Office (BICO) annual survey (2005) states that 83% of the British regard privacy protection as an issue of social importance. The Eurobarometer also states that 70% of EU citizens view the awareness of personal data protection as low.

These surveys do not tell us much. They are limited to separate questions such as: "*Rate how important protecting people's personal information is on a scale of 1 to 5*" (BICO, 2005). The survey does not pose the dilemmas that individuals face in real life, where the individual must make such choices as to give up a little privacy to gain financial benefits (e.g. consumer loyalty cards). Or increased camera surveillance in public transport to feel safer.

The British Information Commissioner stated in an interview with The Times (Ford, 2004) that the country is "sleepwalking into a surveillance society." His concerns, in this case, were the growth of governmental databases on the countries

inhabitants. He stated that when the government has detailed information on its citizens then the government would have the potential to get too powerful in comparison with its citizens. He regards the task of the BICO is to ensure that the government does not gather unnecessary information. In the same article the spokesman of the UK Liberal Democrats raises his concern of the proliferation of databases. Even though each new database can be justified, they can be connected and eventually create a Big Brother society (ibid.).

The concerns regarding the state's information with respect to its citizens can easily be extended to the industry. Commercial firms gather information about their customers from their own relation with them, and they even buy and sell information to create a better picture of their customers.

In 2003, the same year as the latest Eurobarometer, Tulloch and Lupton published their research on risk in everyday life. Their book was based on 134 interviews in Britain and Australia. Their questions related to how people defined risk, dealt with risk and which risks they chose to take and which to avoid. Tulloch and Lupton used Beck's approach to risk on a global, local and private level. The interviewees were taken from a wide range of age groups, sexual orientation, occupations, and educational levels. The interviewees were from Australia and Great Britain (Tulloch & Lupton, 2003).

The most interesting find relating to the aspect of privacy issues in Tulloch and Lupton's (2003) survey were that not a single interviewee uttered privacy concerns. This does not match with the British survey's claim that 83% of the population were concerned about privacy. The same survey states that 83% of the population are concerned with the National Health Services, and health is widely discussed in Tulloch and Lupton's research.

The Norwegian Data Protection Agency (NDPA) cited two surveys in their 2006 report on privacy. The first stated that 3 out of 5 Norwegians believe that privacy is well protected and to surrender information poses no problem. The other survey focused on privacy issues in the industries. By law, businesses are required to establish a system for internal control, define how information gathered should be used, evaluate the risk involved with storing and processing the information and delete old information. Only 4% of the businesses asked complied with these demands (NDPA, 2006).

NDPA's (2006) surveys quoted that 1 out of 6 have experience of personal information having been misused. These people were less trustful than the average. Only in one area were the majority concerned about their privacy, this is on the Internet. Four out of 5 worried that information gathered when shopping on (or using) Internet sites would be stored over time and transferred to a 3rd party.

Former minister of education and research in Norway, Kristin Clemet, calls out for protecting privacy with the constitution, not just common law. She stated that the rewards we receive for giving away some privacy often feel tangible and necessary, while the loss of privacy seems negligible in the short run. By protecting privacy the people will be protected not only against commercial interests, but also against the state itself. The judicial branch can more efficiently stop threats against privacy (Clemet, 2006).

2.3.2. Privacy in an AmI World

In one of the previous examples where the cars are being re-routed from an accident site, AmI provides a tangible, useful feature. It does however require that a road management system communicate with the cars route planning system. The car has to

disclose to some extent where it is going. The user in this example discloses some privacy.

One of the major obstacles in AmI is just how should privacy and security issues be handled. Brey (2005) describes the central idea behind AmI as a concept where computers are ubiquitous, invisible and proactive. The proactive part refers to an ability to initiate communication with other devices. This produces a society where the user either has to constantly choose which smart objects to connect to, or let a software agent choose. In the first scenario the user will grow tired of always being prompted, while in the latter case the user will let a device decide who should be allowed to receive how much information. Brey (2005) also asks if an automatic choice made by a device will truly be based on the users wishes, or if the constructor of the device, or another 3rd party, will affect the choice. The user could easily be in a situation where they have to trust the preconfigured privacy setting in a smart object.

Langheinrich (2001) raises the question on whether or not the users have a realistic choice to protect their privacy? His metaphor is a public building where one must agree to unacceptable practices in order to enter. Is it really possible to walk away? Most supermarkets in urban environments feature video surveillance. A realistic alternative to purchase food without being filmed does not exist. Although video surveillance is closely regulated in most legal systems it does take away some privacy. Langheinrich (2001) states that in order to create AmI devices that protect privacy the user must be able to turn off features that are unwanted without being locked out of the whole system.

Johann Cas (in Casert, 2001) asks if privacy in a pervasive computing environment is a contradiction in terms? The citizens in an AmI world must assume that all is stored and seen. His statement goes on to dismissing laws, regulations and

encryption techniques as methods of protecting privacy. His argument for this is that an AmI environment where privacy is taken seriously is reduced to isolated applications since the information exchange between smart objects will be limited.

Some views of privacy are summarised in Langheinrich (2001). The CEO of Sun Corporation, Scott McNealy, states: "*You already have zero-privacy anyway, get over it.*" While former head of Advanced Research at British Telecom Laboratories, Peter Cochran, claims that we have not enjoyed total anonymity in the world of paper and cannot expect to have anonymity in a world of bits. Amitai Etzioni, from George Washington University, claims that if less privacy helps in providing treatment at an early stage of a disease and prevents crime/terror then the gain is greater than the loss and should therefore be accepted. Computer security researchers Adams and Sasses (2001, p. 2) believe that such views are simply misguided. Their theories will be presented further in the next chapter.

These statements only show that the discussion on privacy is needed early in the development process of AmI. Especially within the medical field where patient information is considered sacred should one recognise the 2400-year-old Hippocratic oath: "*I will respect the secrets that are confided in me, even after the patient has died."* (World Medical Association, 1948)

2.3.3. Two Challenges in AmI

Between the myriad of challenges and barriers of AmI two stans out, namely profiling and data mining. Both are a result of information being gathered and the effect is that privacy is misused. However, none of these are illegal or immoral, it all depends to what extent the methods are used. Profiling is originally a marketing tool, a tool for knowing what a customer might want. The data gathered might be from ones own experience and dealings with a customer but also based on data from other sources,

purchased or traded data. Profiling can be beneficial in some instances, but must not be taken too far. Profiling based on old or inaccurate data can result in unwanted and unpleasant situations for a customer or even denial of service. Profiling, and the data mining that is related to it, can be used to give better service and security but also for surveillance or for bombarding individuals with advertising (Friedewald et al., 2005, p. 46). Both governments and corporations have used data mining tools and profiling to abuse personal information (Friedewald et al., 2005, p. 68). Data mining is systematic collecting and linking personal data and can be a consequence of the continuously rising number of databases that contain information about persons (Blarkom et. al., 2003, p. 197).

When a large part of our lives are tracked, stored and processed the data has to be protected by the data gatherers. The increasing number of databases that are connected creates certain challenges. Data has to be protected but simultaneously shared with those that have rightful access to them. Just by opening databases for sharing data with legitimate users also enables the possibility of misuse by those that are prohibited from rightful access. Data that is stolen can be used to impersonate people in order to obtain loans or other advantages. Data can also be sold to organisations that are not entitled the information. The potential usage of personal data is limited only by the imagination, thus speculating further in the possibilities here is not necessary. While it is easy to discover that a physical object is missing, it is difficult to control that data has not been copied. I will describe these challenges in relation to the SensorPhone in the next chapter.

2.4. Concluding Remarks

In this chapter I have described Ambient Intelligence as a computer system based on intuitive interface and human needs. The discussion surrounding AmI in this paper

has mostly been on a European level and has been presented through the views of researchers, but also to a small degree governments and the industry.

As a step in this thesis I will define the AmI concept based on the literature presented here. AmI will consist of specialised devises and sensors that communicate with other relevant devices and a larger system. It will be integrated into standard objects and is unobtrusive. AmI will gather information, learn about the user(s) preferences and give feedback when due. It should be proactive in its communication with other AmI devises and have the ability to make choices based on the users preferences. Further it should promote human contact, not exclude or replace it. But most importantly its interfaces and actions shall always be human centred.

By narrowing the field from AmI in general towards health issues and privacy related topics I have presented some views that I will return to in the case study presented my analysis. It should be clear now that AmI proposes new methods in treatment and care, and that these new methods pose some obstacles, especially when it comes to maintaining the privacy of patient. Industrialists and researchers are debating heavily on how privacy should be treated in the future, with views ranging from no *privacy exists* to *privacy is sacred*. One element however is clear, and that is that the awareness of the general publics' to privacy issues is low. AmI proposes new methods of providing health care by using sensors and devices to measure bodily functions in a telecare system. The challenge here is to maintain privacy when there are large electronic communication and processing systems involved.

In the next chapter I will present my case study, the SensorPhone, which is in my view, one step on the road to AmI. It is also one step that I believe will help improve life for a group of people.

[3] These interfaces can include, but are not limited to, screens, lights, sound, motion etc.
[4] Gringsby & Sanders mention space shuttles, peacekeeping missions, Canada's remote maritime provinces and Norway above the artic circle as examples of remote areas where telemedicine has been proven feasible.

3. The SensorPhone Case

To be able to show how Ambient Intelligence and privacy issues can interact I will use one of Vodafone Netherlands research programs, the SensorPhone. Even though the SensorPhone will not be a true AmI device, this will be discussed further in part 3.2.

The background for this project is expectancies on how health care will be organised in the next three decades. An emerging field of biomedical sensors combined with modern technology and wireless communication will enable a more efficient delivery of health-care. By combining existing technology one can promote new, innovative applications and services by transferring tasks and competences of the human doctors to automated devices.

The focus of the SensorPhone project is to develop and validate a health service centred on the collection, transmission and analysis of data from a wearable wireless 3-axis accelerometer. Gathering and transmitting data from the accelerometers to a clinical service through a standard mobile phone can enable high quality feedback on movement to the user. In this study the focus is on delivering information on calorie expenditure and exercise patterns to obesity patients (Vodafone, 2005). The obesity group is chosen because that group will benefit greatly from movement/exercise and also because of the growing concern regarding obesity in society. The vision is that the project should be extended with a wide range of movement and medical sensors thus enabling it to treat many different diseases and conditions. One goal for the research project is to field test the equipment on approximately 30 test subjects when the first edition of the technical components is built.

It is unclear at this stage of development if Vodafone Group will ever develop this project to a final stage. They might develop it further in-house, outsource, sell the project or even cancel the project. Vodafone is primarily a telecommunication company, not a medical supplier. However they have developed and are currently marketing health related applications[5].

3.1. Description of the System

Since the SensorPhone system is not yet a finished pruduct, but a research project at Vodafone R&D; a complete and final description is not possible. I can however describe how it is intended to look at this stage. I will start my description on the level closest to the future user and follow the intended dataflow from there on. The description is based on internal project documentation and conversations with Vodafone personnel and external researchers working on the SensorPhone.

The Sensors: The sensors in the system that gather data will be unobtrusive, and attachable directly to the body, on clothes or purpose built bands to possibly be worn at all times during the day. The first sensors will gather movement data and transmit to a data acquisition and analysis device (DAA) using wireless low power - low range protocols. At a later stage, sensors that gather data regarding blood pressure, heart frequency, EMG, glucose concentration, insulin and other medical information will be considered for addition. The latter stage can also include sensors that measure non-body movement or functions, such as a bike-monitor, measuring speed and distance.

Databutton: The databutton or Data Acquisition and Analysis device (DAA), as it is also called, is used to gather information from the sensors worn on the body, store it, perform basic analysis and transmit it. The level of analysis (depending on memory requirements, processing power and battery life) and method of transmission

(to a mobile phone or directly to the phone network) is still to be determined. This device must be in close range with the sensors to gather data therefore it should fit in a pocket or be attachable to a belt.

Mobile phone: A standard, off the shelf, GPRS/UMTS mobile phone will most likely be used to transmit data from the Databutton and to the network. The phone will be fitted with special software to handle SensorPhone tasks. To communicate with the Databutton it will use the Bluetooth transmission protocol. The system will use a special SIM-card in the phone with encryption capabilities to create a secure data-transmission. Additionally the phone will have SensorPhone software that will present feedback, reminders and motivational messages from the system to the user in an appropriate format. It is the wish from Vodafone that the system should work on most low-end phones.

Processing and storage: The data from the sensors is processed, stored and made available to certain functions. These functions can include a SensorPhone medical call centre that will be assigned the task of providing feedback and medical advice to the users and potential caregivers through various channels[6]. The feedback can be generated both automatically and manually. It will be possible to share data with other parties from this point. One of the advantages of the SensorPhone is the ability to deliver high quality data on the users health to a physician (by the consent of the user).

Website: Due to limitations on the screen of a mobile telephone there will be included a website in the system where users can receive more detailed and customised feedback on their status. The website also has the potential to show more general advise regarding the users condition, nutrition and physical activity and to connect the user to other people in the same situation. To log onto this website and

view personal information then the user will need to go through an authentication process to ensure that the inquiry is legit.

Physician: When the system is used for treatment the physician will still be the one responsible for the medical effort. Together with the patient the physician will set both short- and long term goals for treatment. The physician will have the opportunity to continuously monitor the patient and give feedback when needed.

Other: There might also be a more generic customer service centre that will be tied to the phone subscription. Further, technical staff and administrators will also have access to data to be able to perform updates and maintenance work required to run such a system.

Figure 1: The Body Area Network.

Figure 1 shows the elements of the SensorPhone that the user will wear in what Vodafone has named a Body Area Network. While the sensors do not have a storage capacity and will need to transmit continuously to the DAA, the DAA can store and process data and need only periodically be attached to the mobile phone.

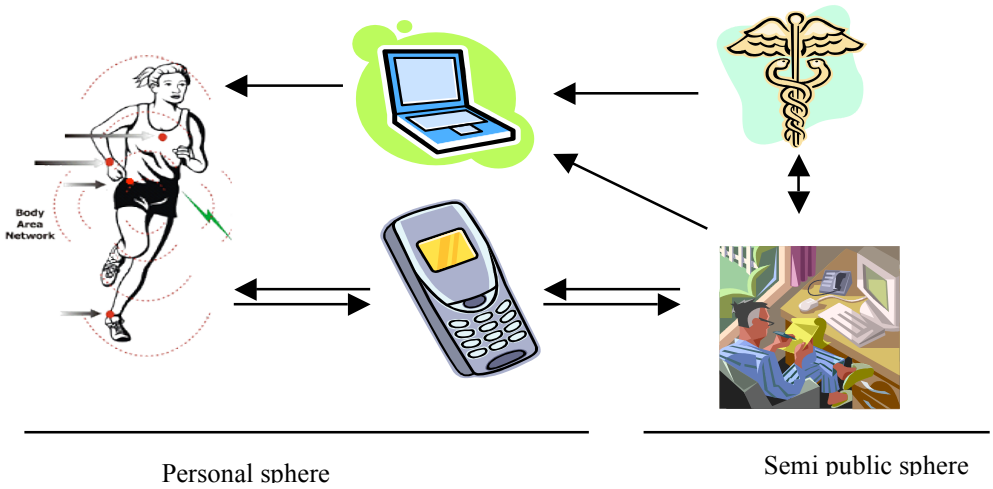


Figure 2: Rough outline of the intended dataflow in the SensorPhone system. The databutton is not shown but should have been between the user and the cell phone.

Figure 2 shows the dataflow in SensorPhone. Movement data is transmitted from the sensors continuously and received by the databutton, which stores and processes it. The databutton then sends information to the cell phone that can display a health status and forward the data to the processing and storage at the call centre. This centre produces more detailed reports for the physician and for the user that can be reviewed on a web page.

3.1.1. Three Different Uses of the SensorPhone

As I have mentioned earlier, the intention is to test the SensorPhone system on obesity patients and that this group will be the first users. The reason for choosing this group is that there is a growing number of obese people in society. Obesities have reached epidemic proportions in the United States and other industrialised nations (Poston & Foyet, 2000). Being overweight is the result of a chronically positive energy balance as intake exceeds consumption. Since the system measures movement, and encourages the user to more movement, thus raising energy consumption, it is suitable for obesity treatment.

Parallel to the development aimed towards clinical treatment there is research within Vodafone to see if the system can be used as a personal fitness and health application. The same sensors, DAA and phone can be used in such a setting, but with a slightly different focus in the software and website.

One of the major differences between those two groups is that the obesity patient should wear the system throughout the day to track the total calorie expenditure and exercise level. While with the fitness users it is enough to wear it when exercising, although they can wear it throughout the day as well. The need for sharing data with a physician in the fitness domain is considered less important than in the treatment domain. The goal of the SensorPhone in both these cases is to encourage more movement.

A third potential user group emerged as the project has evolved. That is the use of the SensorPhone as a tool for medical diagnostics. If a doctor attaches a range of medical sensors to a patient, who will wear the sensors (with the rest of the system) for a period of 24-48 hours the doctor can get high quality data on the health condition of the patient. As an example, the doctor could see how the blood pressure changes throughout the patients' normal day, instead of just a sample when the patient visits the physicians' office. A legitimate question here would be, who is the user? The patient wears the system, but the doctor is the one who reviews the data. Since it is the patient's data that is at stake, and this paper looks at the privacy aspect I will consider the patient as the user.

3.2. The SensorPhone as an AmI Device

I started the previous chapter by stating that AmI would not suddenly be invented but would rather be a convergence of technologies. In addition this chapter began by

stating that SensorPhone is not a true AmI device. What are then the similarities and differences between AmI and SensorPhone?

The sensors and databutton will be specialised devices. Programmed to perform a limited set of tasks and to communicate with the SensorPhone system. They will be as unobtrusive as possible, but will not be integrated into standard objects. The exception here is the SIM-card and software that resides within the mobile phone, which is a standard object.

The learning aspect is debatable, the system gathers and stores information about the user, but is that learning? Learning will often imply knowledge, not just holding information. If the system consisted of purely technical elements it would be hard to imagine new connections and correlations being found. But there are people in the system as well, maintaining and developing the system further. These people can add new algorithms into the SensorPhone this would increase functionality, and therefore infer that a degree of learning is present in the system.

One of the key elements of the SensorPhone is that it can give feedback in response to the level of movement. The feedback should also reflect the needs of the user, giving the preferred amount of information at the preferred time.

The arguments above imply that the SensorPhone as an AmI device, at the present however, I will reserve judgement. My reason for this is that the SensorPhone does not connect to devices outside its specific frame[7]. It does not make choices based on the users preferences either. Further, it does not directly promote human contact, since the patient – doctor communication is mediated through machines. Even though a human physician can send messages through the system the interface is a machine. This, has of course two sides, the users does not have to use time to travel back and

forth to the doctor, freeing up time to spend with friends and family. At the same time one misses a close personal connection to a doctor.

In a true AmI world, the goal is that everything should be connected. The SensorPhone is targeted to a limited segment, in the first stage, these being obesity patients and fitness interested. However, due to the partial fulfilment of the AmI requirements I will claim is that SensorPhone is a step on the way towards AmI technology.

To summarise the similarities and differences between AmI and the SensorPhone see the table below:

Defining AmI:	*SensorPhone specific:*
• Specialised sensors	Yes
• Communicate with many	No, only preset entities.
• Part of a larger system	Yes, part of health records and treatment.
• Integrated into standard objects	Partly, Sensors and DAA are specialised objects.
• Unobtrusive	Partly
• Gather information	Yes
• Learn about users preferences	Yes
• Provide feedback	Yes
• Make choices	No
• Promote human contact	No, not directly.
• Human centred interface	Aims towards it, but yet to see in reality.

3.3. Threats to the SensorPhone

Some of the SensorPhone is key characteristics is its ability to share data. However, this sharing should always occur within the system, between the user, call centre, system administrators and the potential doctor. After carefully reviewing of AmI

literature, with the aspect of privacy in mind, my claim is that the largest threats to the SensorPhone are profiling and data theft.

Profiling is not an illegal or immoral activity, it is a market tool to analyse customers and their need. It is done on a daily basis by most organisations that on some level have customer or user data. As mentioned in the previous chapter, it is an important tool for organisations to know their customers. Although profiling used to its full potential can feel intrusive for the individual since it will seem that the organisation knows the individual too well. Some effects of extensive profiling can be identification and cancellation of customers that will potentially be "troublesome" in the future. Simultaneously creating strong lock-in functions to keep the attractive customers with the expense of a healthy competitive environment.

One can easily imagine that data from the SensorPhone can be interesting for a number of organisations. The users medical insurer has a monetary interest in knowing if the program is being followed. A users failure to follow SensorPhone recommendations might increase the risk that the insurer must cover medical expenses. Hence, not following SensorPhone recommendations might increase the insurance premium for the user if the insurer can track the progress. Other unwanted results of profiling can be an increase of unwanted direct marketing (through mail, e-mail, phone etc).

Data theft is a threat to privacy in the SensorPhone due to the sensitive nature of health records. This is especially true for the treatment usage, where data is gathered over time and the progress can be seen, and in the diagnostic usage where a large number of sensors can describe the health situation very accurately. This data can be valuable for the insurance company as described above, but also a wide range of other organisations and individuals. To draw a parallel, in July 2005 stories about

the sale of phone records featured headlines in the United States. Through websites, companies offered to sell phone records to anyone with a credit card. The data was most likely stolen from the phone companies by either unfaithful employees or by someone impersonating the phone account owner (Krim, 2005). To receive data about the last hundred calls of General Wesley, former presidential candidate and former head of NATO took less than one day and cost $89.95 (Potter, 2005). Clearly, such services are unwanted by the general public and a similar service with health data would be a clear and extreme violation of privacy rules and wants.

If data from the SensorPhone became equally available one could check the medical status of colleagues, neighbours and friends with the tap of a button. Newspapers and scandal magazines could provide lists of celebrities and politicians together with the conditions they are treated for. A data thief could even blackmail a user to pay money for not making data public. This is of course a rather pesimistic view, but it should be discussed so that proper safeguards can be implemented.

Profiling and data theft can be tied together. The logic here is that one organisation that wishes to use profiling as a tool can use data gathered illegally, either by themselves or by a third party. The source for this data can be employees of the organisation where the data originates or hacking into a system.

A threat that is present and potentially harmful to the individual is theft or loss of the phone with the data it contains. Even though a thief potentially could access the data it is more likely that the phone, not its data, is the target for the theft. Even if the data were taken, that would only affect one individual. In comparison, data theft and profiling could harm the whole customer base of the SensorPhone.

3.4. Summary

The SensorPhone is as mentioned a research project at this stage. The focus in the project is to establish a working connection from sensors to the mobile network and interpret the data in a meaningful way to be able to create a useful, marketable product. The components and target groups in the system might be altered when changing it from a research project to a product. One element of the product that will not change is that SensorPhone uses sensors to gather data regarding the user and that the data will be processed to provide feedback on motion / bodily functions. There is a potential threat to privacy by extinctive profiling by Vodafone or partners, and theft of data resulting in unwanted organisations knowing too much about the citizens.

---

[5] Vodafone Biozoom is an example here, a scanner that measures enzyme levels, water levels and body fat percentage and transmits it to a mobile phone. The Biozoom is due to launch in late 2006, but will probably not use Vodafone as a brand name (Vodafone 2006a)

[6] These feedback channels can include, but are not limited to, the phones screen in the form of text and graphs, voice communication, periodical reports, a website.

[7] Here I separate between the SensorPhone part of the mobile phone and its other functions.

4. Theoretical Framework, Privacy and Functionality

4.1. A Model for Privacy Assessment

To be able to assess how the public perceive privacy I will look towards Adams and Sasses' (2001) work on privacy in the field of multimedia communication. Their angle of research is audio- and videoconference communication but it can be extended to include privacy issues in most technological settings. In their view multimedia communication is a positive form of communicating, however it also brings risks in the form of lost privacy. The communication can be stored for an unknown period of time, the full list of recipients is not always known and the persons recorded can rarely control the usage of the stored material. The user will have some perception on what data is being collected and what it is being used for. If an assumption makes this perception wrong then the user will experience an emotive reaction, their trust in the technology will decrease and the technology can be rejected.

In my opinion the method and model described in this chapter should be used when building the SensorPhone into a marketable product to assess the privacy aspects of it. The model should also be relevant when developing other Vodafone products and services. Due to the mobile market in the Netherlands, as with much of Europe, being fully saturated the development of unique products and services is a strong tool to keep customers. Many new services cross the boundaries traditional of the person to mobile phone relation, gathering data about the user, utilises several mediums and often several organisations that complement each other will be involved. The model described can be used to investigate how the potential user approaches and views the elements that consist within a new product or service.

4.2. Two Opinions on Information Sensitivity

A challenge with privacy is the existence of expert- and lay dichotomy, and that these opinions can differ greatly. In the case of SensorPhone and privacy, we can acknowledge the legal- and the IT-security departments within Vodafone as experts, while other departments and future users can be considered lay-people. The expert opinion, is based on rationalism and private information can include items such as social security number, credit card number, tax records, medical information etc, i.e. information that is private by law. The general notion is that experts are supposed to be knowledgeable and the laypersons are ignorant (e.g. Maranta et al., 2003, p. 105). This is traditional view is reflected in some of the experts within Vodafone who believes that the majority of their customers (laypersons) are not concerned with privacy (Interviewee 3 & 4). However, at the same time they recognise that there are privacy experts, or concerned laypersons, outside of their organisation as well (Interviewee 4). The notion seems to be that if the experts within Vodafone can satisfy the experts outside Vodafone then the laypersons should also be satisfied.

The layperson will think of most items considered private by law as private, but they can also include other information based more on emotions, such as the amount of chocolate consumed in a week to use a blunt example. The expert will most often have a rational approach to what is private data, while the individual will often use emotions to determine the level of privacy in each setting (Adams & Sasse, 2001). The perception of the situation and culture will be the main factors that determine what an individual is ready to reveal about themselves. The experts in Vodafone should therefore analyse what data is gathered by a SensorPhone system and then include laypersons in deciding what is acceptable and how data should be treated since the laypersons are experts in what they are willing to accept. This would

assure that the designers of SensorPhone do not rely solely on the requirements of the law and security standards but also on the future users.

4.3. The Model

To identify which data the user regards as private, for whom, for which usage and in which context Adams and Sasse (2001) developed the privacy invasion model. The model is based on grounded theory from sociology, and was developed after reviewing privacy literature and phenomena within multimedia communication (Adams & Sasse, 2001, p. 3)

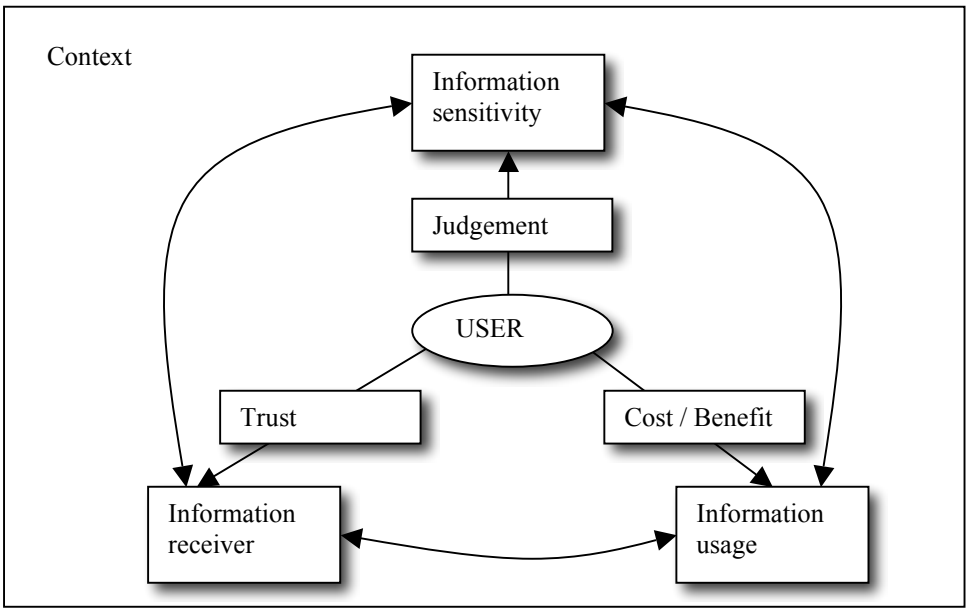


Figure 3: Privacy factors and issues (Adams & Sasse 2001)

Adams and Sasses model show the factors the user considers when dealing with privacy issues in a technological setting, and how these factors interact. These factors will be the main elements of the analysis I will perform in this chapter. These elements should also be taken into account when analysing privacy aspects of functionality into the SensorPhone.

This mental model deals with the users perception of the context, receiver, sensitivity and usage. This perception can be incorrect, biased and incomplete, but it is with that perception the user will approach a technology (Adams & Sasse, 2001, p. 5). The challenge Vodafone faces is to identify and close gaps between negative perceptions and reality.

4.4. Vodafone's View of the User

4.4.1. The Context

The context in which SensorPhone operates in the first stage will be with one of two groups of people. The first being with an obese person with a wish to cure a chronic disease. SensorPhone will then be one of the choices of treatment, alternative medical choices will be medication, surgery or cognitive therapy. The second context will be a person with a general interest in health that views SensorPhone as a better option than other exercise schemes.

When the SensorPhone is operational it will gather movement data and it will give medical and fitness related feedback. In the case of obesity the data can be shared with health personnel and can become a permanent record in an electronic patient journal. The system can manage a schedule of activities that the user and physician have agreed upon. If a scheduled activity is neglected it can remind the user, and potentially the physician. The intention is that the feedback given should be part automated and part by the physician. The possibility of frequent feedback is considered by Vodafone to be one of the major advantages over the previous paper-based system. It can stimulate a closer doctor – patient relationship, even without the patient actually spending time to travel to the doctor and back frequently.

A part of the context should be how Vodafone customers view privacy at present. Several of the interviewees stated that the regular users of Vodafone services are not concerned about privacy. Interviewee 3 believed that their customers view telecommunication companies as black boxes, they are not aware of what can go wrong. Further he claimed that large corporate customers ask for meticulous security of their data, while individual consumers mainly do not care. While Interviewee 5 claimed that not many users ask about how privacy is maintained, possibly since misuse of information is not a major problem. In addition the NDPA yearly report states that people seem to prefer easy electronic solutions to problems and that the demand for anonymous solutions seems low (2006, p. 14).

It is difficult to predict the future, but the general publics awareness of privacy may increase in the coming years as a result of more intrusive elements. After reviewing the literature on privacy my claim is that the trend seems to be that people that have been, or know people that have been, the victim of identity theft or have had other negative experiences with breaches of privacy becomes more cautious (e.g. NDAB ,2006). Privacy intrusion is also on the rise, most notable by identity theft, but also by gigantic databases that are being built[8]. The effect of this is that Vodafone should implement strong privacy protection into their systems. In my view strong protection can not only be demanded at some stage by the consumers but can then also be used as a strong selling point for Vodafone. Overall it should also require less effort to build a strong system for privacy protection from the start than implementing it into SensorPhone some years later.

4.4.2. The Judgement on the Sensitivity

The users will determine what information they regard as sensitive. In combination with the law, their opinion will form how Vodafone determines what SensorPhone

will regard as sensitive. Vodafone can choose not to follow the law or user demands, but the consequences, if detected, can be devastating in the form of decreasing reputation and loss of customer trust.

Adams and Sasse (2001, p. 6) found that information has at least two levels. The first level is the core data where the data is collected to fulfil a certain pre-agreed task. The second level is other social and psychological interpretations that the data can be used for. Adams and Sasse found that users would feel that their privacy has been invaded when they assume that data has been used on the second level in a way not anticipated.

To decrease the possibility that the user will experience a privacy invasion with the SensorPhone Interviewee 4 is of the opinion that a clear contract will have to be made between supplier and user, showing the dataflow and which parties are involved[9]. This will clarify for the user, what data is gathered and how it is processed, thus closing the gap between perceived and real usage of data.

Sensitivity is also situation dependent, not only related to a private or public place. One can imagine that the user does not want all his or her actions and tasks to be recorded, thus there should be a realistic option to switch off the SensorPhone when wanted without a major loss of functionality.

Interviewee 2 did not believe that privacy was a very important part in the mobile communication, referring to studies showing that mobile users have no troubles talking loudly about subjects otherwise considered private in a public place. Although, Interviewee 2 did admit that it could be different when it relates to transmitting health data through the phone. Here we can question whether one is in a private situation when on a bus. When among strangers, one enjoys a certain level of anonymity.

The opinion of Interviewee 4 is that among the potential SensorPhone users there will be many who do not care about the privacy and sensitivity of the data it produced. However even if only a small minority care about where the data goes and what it is used for, then Interviewee 4 would like to cater to their wishes, whereas by supplying all the users with the same level of data protection.

Interviewee 4 goes on to state that data gathered by the SensorPhone will very easily be considered sensitive health data by the law, and thus legally require a strong data protection regime. The data from SensorPhone can, at some point, be integrated into the electronic healthcare record that is now under development in several EU countries. An integration of SensorPhone data with other health information regarding the user increases the functionality since the physician can follow the patient's whole history. One key obstacle for the SensorPhone is that it must be accepted by the medical community, to be accepted SensorPhone will have to follow the standards the medical community use. Therefore the SensorPhone should be considered as health data and given the strong data protection required for health data.

4.4.3. The Cost and Benefit of the Usage

The cost and benefit of SensorPhone can be viewed in several different ways. To be able to get access to the system a monetary cost has to be paid by the user, insurer or state to the producer. Cost is not only a monetary function; it is also a metaphor that implies having to give something up, with a negative connotation. Therefore, it is possible to view the loss of privacy that the user experiences as a cost. There will always be some loss of privacy when using a system like SensorPhone since data is gathered and shared beyond the immediate control of the user.

The cost alone is not enough to analyse SensorPhone by, one must also look at the benefit from using the system. The benefit will be different for the different

segments. The fitness interested might view it as a novel gadget that adds a bit of flavour to the daily exercise, while for the obese patient it can literally be a lifesaver. Following this logic it is reasonable to believe that the total cost acceptance is different for the two segments.

Interviewee 3 compares SensorPhone with loyalty cards issued by stores, and recons that most people will not have a problem with giving up a little privacy if they gain an advantage, however small the incentive will be. Cochran shows a utilitarian view when he claims that easy access to medical journals can save life (Langheinrich, 2001, p. 5). Following his view the cost of privacy is little compared to the benefit of saving life. Interviewee 3 follows Cochran's thoughts when he foresees a SensorPhone that detects a possible heart attack as a side effect of its usual measurement. Then all efforts should be used to save life regardless of privacy laws and regulations. The dilemma here is that easy access to medical journals in a life-threatening situation also provides easy access when not in such a situation.

Interviewee 3 states that security, from a Vodafone perspective, is always seen in a business context and privacy protection as a matter of diminishing returns. The end-user eventually has to pay for the cost of adding extra protection and one will reach a stage where the customer does not want to pay more as the cost outweighs the perceived security gain. This will happen before total security is reached. A computerised system that is one hundred percent secure is unobtainable with today's technology and organisational systems.

4.4.4. The Trust in the Receiver of the Data

The third privacy factor is trust in the data receiver; trust itself is a complex issue within e.g. the fields of sociology, psychology and business. Adams and Sasse describe trust as a user's perception of a person. The person can here be a metaphor

for e.g. a business. Trust is a function of relationships, information roles and group membership (Adams & Sasse 2001, p. 8).

The general public only associates Vodafone with voice telecommunication, not as a supplier of medical devices (Interviewee 5). In addition the BICO survey states that only 20% of the British population trust a telecommunication company to take proper care of personal information (BICO 2005, p. 13). Then how can they work with sensitive health information? The concern here is well founded. A suspicion from the buyer that the seller is not capable to fulfil its promises due to lack of expertise is a strong threat to the buyer - seller relationship (Doney & Cannon, 1997). Vodafone's credibility as a mobile operator might be high, but they have no credibility as a medical supplier. Hence the group membership that the general public associates Vodafone with is not a highly trusted group, and is not related to the trusted medical group.

According to Interviewee 5 it might be easier to launch a new brand rather than trying to rebrand Vodafone. Creating an own branded identity follows the view of corporate communication principles when the two markets are different. When Vodafone tries to market itselves as "Young, Fit & Fun" it will be difficult to sell medical applications with that identity. Although, a logo stating that Vodafone carries out the data transmission might be beneficial since Vodafone is associated with telecommunication. In this case it would be an endorsed brand where parts of the identity of the mother brand are transferred into the subsidiary (Riel, 1992).

Interviewee 1 suggests that a medical doctor should prescribe the usage of SensorPhone to relevant patients. If a physician proposes SensorPhone as part of a treatment to a patient the doctor includes SensorPhone into the medical group, and

SensorPhone can enjoy that groups credibility. Such a referral system can increase the overall users trust in SensorPhone.

When I first met with Interviewee 1, I was told that they would implement a Liberty Alliance[10] security structure, at least during the research project, to keep data safe. If they continue to use the Liberty Alliance, or any other security structure they need to communicate to their users that their data is being protected, and how it is protected. Interviewee 4 would want to have a very detailed contract between Vodafone and The SensorPhone user. Her claim is that Vodafone must be extremely clear in its communication with the user on what the data is being used for, where it goes, who uses it, and most importantly that it never leaves the chain. Interviewee 2, on the other hand claims that people want to know if their information is secure, but they do not want to read lengthy legal disclaimers or contracts. A detailed contract contradicts clear communication since contracts are often lengthy and written with a judicial language.

My initial solution to these contradictory views was a trust building seal to use on the products and in marketing as a guarantee that the SensorPhone follows a set of rules regarding privacy protection. A similar seal to the eco-labels *die grüne punkt* or EU's *The Flower*[11]. Such a seal would be issued by a trusted and neutral 3rd party and be anchored in the general publics mind to have a trust transferring function. The criteria could be stated as an ISO standard with audit requirements as suggested by e.g. Blarkom et. al. (2003). However, the effect that such a seal has on customers is debatable and no final conclusion has been agreed upon. Riegelsberger & Sasses (2001) research on trust in online stores suggest that such a seal has limited use while Hu et al. (2003) documented some positive effect of a seal. Most notable, is that a familiar seal on an unknown storefront increases the willingness to buy. More

research should be done on this, due to its potential to translate a complex set of demands into an easy to understand graphical symbol. Other industrial actors that create complex products and services should be equally interested in trust enhancing seals. A joint effort in the industry to set up an organisation to handle the seal or lobby activities towards the government should be considered in order to develop a seal.

Remarks from Interviewee 2 on the dataflow indicate that the system should be very transparent relating to how movement of the sensors are translated into recommendations. By visualising this translation for the user, the user will perceive a more personal ownership of the data and their trust in the treatment will probably increase (Interviewee 2). Punie et al. (2005, p. 42) agrees on this view and claims that by showing the user how the system operates the feeling of uneasiness and loss of control can be avoided. While not directly related to privacy, such transparency can aid in increasing trust in the system as a whole.

4.5. Privacy Invasion Cycle

The outcome of the privacy factor model is the privacy invasion cycle (see figure 3). A model that explains the reaction the user will have if their assumptions on the technology are perceived to be wrong. The reactions of the user will be on an emotional level, based on assumptions, and the outcome can be a rejection of the technology and decreased trust in the organisation that delivers it. A previous experience where technology has been rejected due to privacy concerns will also be part of the evaluation process when considering a new, similar technology.

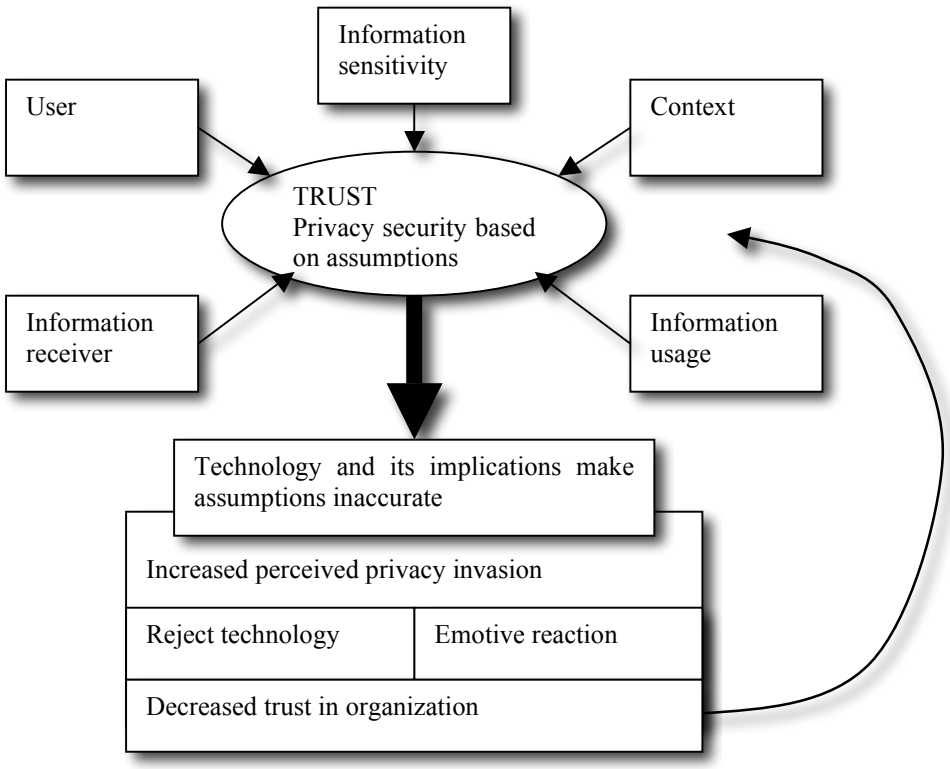


Figure 3: Privacy invasion cycle (Adams & Sasse 2001)

Adams and Sasse (2001, p. 15) propose this model as a valuable tool to analyse potential privacy problems and counteract them before they arise. To analyse each function for each segment of the SensorPhone with this model Vodafone can solve how the potential customers perceive their privacy and prevent loss of trust and emotional rejection of the system.

4.6. SensorPhone Scenarios

With the description of how the SensorPhone system might be built in the previous chapter and the description of Adams and Sasses privacy models in this chapter one can build scenarios for how Vodafone should address the privacy versus functionality issue. The main goal that the SensorPhone should achieve is as previously noted to monitor movement and provide feedback on that movement. This can be done on

several levels in the system; each level will provide a different set of functionality and privacy intrusion. I have created the three following scenarios to illustrate different levels of functionality and privacy in obesity treatment in a SensorPhone environment.

Scenario one would be local processing of data and feedback based solely on software in the databutton and mobile phone, thus leaving out the connection with a processing and storage facility, a website, physician and other external entities. The feedback here would be reduced to numbers describing the amount of movement (distance moved, speed, calories expended etc). The level of privacy in this scenario is high due to the system being closed and no data is sent from the users handset. However, exercise systems that have this type of functionality are already on the market. The Finish company Polar provides a well known and established system with heart rate monitoring, they also cooperate with the mobile phone producer Nokia to deliver a system that measures heart rate during exercise. The data is transmitted to a Nokia handset for processing and presentation. In addition the Dutch product PAM provides a movement sensor that gives points when moving around; the data can be uploaded to a computer program to track day-to-day progress. If the SensorPhone were to give feedback only at this level it would not give anything new to the market.

In scenario two the data gathered by the movement sensors is transmitted through the databutton and handset to the processing and storage facility. The whole process of reviewing and responding to the information is automated and based on algorithms. This would add the functionality to compare data over a longer period (years) and more processing powers would be utilised to interpret the numbers. There would be no human interpretation. This introduces the risk of data theft on a large scale, either internally or externally. Data spillage, where people get access to the data

unintentionally might also occur[12]. This scenario would bring something new to the market but it does not use the full potential of the SensorPhone.

Scenario three would add human interpretation into the system; this gives the highest level of functionality, but also the biggest risk to privacy. The users doctor and/or a medical call centre would access the data and provide highly personalised feedback on the user's progress. This introduces a larger risk of human error into the system. A wide range of people might get access to it, intentionally or accidentally. Consider the number of people working in a doctors office or the high employee turnover rate usually associated with a call centre, and how many of those can see a patients file either purposely or by accident. This creates a situation where maintaining privacy is difficult.

4.7. Surveying the Test Users

The SensorPhone is currently at a research stage, and will be tested with approximately 30 test subjects to verify that the dataflow and algorithms are fully functional. My recommendation will then be to have in-depth interviews with the subjects before and after the test to survey how they view privacy issues and how this view changes when wearing the system. The topic for the interview should be based on the three privacy elements found in Adams and Sasses model. Such interviews can disclose the difference between how user's lay opinion on sensitivity differs from Vodafone's expert opinion and other differences in the perception of the user and Vodafone's opinion. Vodafone's development of the SensorPhone should then reflect the view of the subjects that are most concerned with privacy if we follow Interviewee 4's wish to accommodate for that group. Such an analysis should use exploratory qualitative, rather than quantitative, methods to uncover the subject's emotions and assumptions. Vodafone can here divide the group of test subjects,

surveying one group before and after the trial, the other one only after. This method can show how much more, if any, the subjects consider privacy when asked about it in the start of the tests (Gripsrud & Olsson, 2000, p. 115-120).

4.8. Conclusion

The potential users of the SensorPhone will evaluate the system before purchase and continuously during usage. The evaluation will be based on the perceived sensitivity of the information, the trust in the receiver of the information and the perceived cost – benefit of the usage. We can acknowledge that users with the highest gain can pay the highest total price, meaning that when the SensorPhone is used as a lifesaver then the user can be willing to give up their privacy in order to be treated. On the other side those who use the device as a supplement to exercise might not be willing to be constantly monitored by external actors. Note here that there is a difference between giving up privacy to a trusted partner and to anyone. The requirement for maintaining privacy is not only required by the wearers of the system, but it is also crucial to be accepted by the medical profession.

The users assumption on how SensorPhone operates dictates whether or not they will use the system. Therefore Vodafone needs to assure that the gap between assumptions and the reality is as small as possible. Including the future users in the design process aids with this. When the system is operational Vodafone should use transparency and contracts to keep users informed on how their data is used and by whom.

Further I would recommend that Vodafone undertake investigations towards a secure environment label together with other industrial actors. By labelling products and services the industry can communicate to the users that their environments maintain a certain level of privacy and security.

Subjects in field tests should be interviewed on privacy and functionality matters to identify the users attitudes towards this issues. This will provide Vodafone with information they can use to build a system that will be acceptable for the largest possible audience.

I would further recommend that the branding of the final product should be done either as an endorsed brand or as its own branded identity. In my view, mixing Vodafone's current corporate identity with a medical product can create an unfavourable situation for both the core business and the medical products.

My finally recommendation will be to start implementing privacy protection at an early stage. If privacy is built into the system from the start and a culture for maintaining privacy is developed then Vodafone will be better suited for facing tomorrow's privacy challenges.

---

[8] E.g. Plans in Great Britain to built databases on every child in the country (Ford 2006) and plans in various EU countries to build large health databases (NICTIZ 2006.)

[9] This statement is on the borderline between this paragraph and the paragraph on trust, I have included it in both but with a different angle.

[10] The Liberty Alliance is a consortium developing methods for protecting identity and data in network devices and services (http://www.projectliberty.org/about/index.php)

[11] For Die grüne punkt see: http://www.gruener-punkt.de/ and for The Flower see http://ec.europa.eu/environment/ecolabel/index_en.htm

[12] E.g. In August 2006 a newspaper found that the search history of users of the American Internet operator AOL were available to the general public. By analysing the search history the journalists were able to track down the users. (Reuters 2006)

5. Inscription of Privacy

When Vodafone develops the different components in the SensorPhone they simultaneously configure a future user. Choices made in the design process affect who the user will be and who will not, how the object will be used and developed further. ANT scholars such as Akrich and Latour employ a semiotic notion of technology as a script where technical objects define a framework of action together with actors and space (Oudshoorn & Pinch, 2005, p. 9). Akrich (ibid.) goes on to suggest that the technologists build a system based on their anticipation of the potential users and the users in their turn act within the frame that the script allows. When the objects are delegated with responsibilities and specific duties then the objects themselves become actors. The real users in their turn participate in deciding how the object will be developed further. Since the SensorPhone system is currently being developed I, as an analyst cannot descript the system, what I can do is make the designers aware of how their inscription, projected user and mediators will affect the system and real user.

In the process of developing this system one will find internal and external groups that will demand certain functions in the system for them to use it. Among the system designers one will find reflexive users, designers who build the system so it can be used in a way they want to use it themselves. Mediators are an external group with special interest in the technological development of the artefact, and are viewed as a group that represents the users as a whole (Lindsay, 2005).

I have earlier in this paper mentioned some threats to the SensorPhone and the maintenance of privacy such as data sharing and profiling, how insurance companies could use data and so forth. In this chapter I will discuss a method for preventing privacy leaks, the authentication process is my example and can be viewed as a

superior method of maintaining morality in the system over e.g. a human staffed call centre. The authentication process becomes a gatekeeper in the system, ensuring that only those who subscribe to the system will be able to view data. While an authentication process protects against external snooping additional efforts are needed against internal threats. Those within the system can have elaborate access, and that access might be needed to be able to perform certain job functions. E.g. the call centre in the system will have a business need to access customer data when users calls in and the computer system administrators need access so that they can ensure that the system is operational. But how can one ensure that the call centre employees do not spend time looking up their neighbours and prevent administrators from providing data to insurance companies?

5.1. Privacy and Morality Delegated to Non-Humans

For some people the notion that devices have morality seem absurd, however ANT scholars argue that morality is indeed part of technology. Verbeek (2006) builds on Latour and Akrich's claim that technology is not strictly functional, but that it also fulfils a manifold of roles within its context. Further Verbeek (ibid.) describes the script approach as a way to look at designers' responsibility for how their technologies act when used. Technologies, according to Verbeek, materialise morality. The designers should assess whether their products have undesirable mediating capacities (ibid.). To use customer data in a way customers do not agree with or view unfavourable to them is then morally bad behaviour. Vodafone faces numerous challenges in proper privacy management.

A much used example in ANT literature of the speed bump as a moralising object in the road illustrates how technology can enforce certain morals onto humans. The humans cannot be trusted to drive slowly therefore technology is prescribed to

force that morality upon the drivers, and punish those who challenge the rules by damaging the suspension on their cars.

The SensorPhone itself is a moralising device, working as a conscious for the user. Constantly trying to alter the user's habits towards a healthier lifestyle by giving the user the message that if they follow the SensorPhone advice their health condition will improve. The SensorPhone is divided into many different sub-systems, one of these is authentication processes which the user has to go through when the SensorPhone sends or retrieves data or when logging onto the website. It should be mentioned that parts of this authentication could be automated, happening in the background on the user's mobile. An authentication process could be similar to the one used when logging onto other websites, such as internet banking or e-mail, one uses a login name and password to identify oneself as a legitimate user of the service. The strength of the security can be determined by the strength of the password requirement. The password can stay the same during the time the user use the SensorPhone, it can be required to be changed on a monthly or yearly basis, or it can even be a unique pin-number retrieved from a device for each log in.

In the SensorPhone case privacy can be inscribed into the system in a visible or an invisible way. In the visible case the screen will show an authentication process when logging onto the system, while in the invisible case everything will happened in the background, hidden from the user's view. Both these options have an effect on the system. Some users might view the visible approach as a hassle, while the hidden approach might make privacy aware users question whether or not there really is an authentication process. Since both Interviewee 3 and 4 recognise that most Vodafone customers are unaware of privacy issues, but that a minority are aware and the Interviewees want to satisfy this group, the authentication process should be visible.

An authentication process on a website that requires not only the users name but also a password can be viewed as a moralising process. The process is inscribed with a suspicion that the one trying to use the service may not be the one he or she claims to be. A secret password that is agreed on between the provider and user secures that the user John Smith is in reality John Smith, not just someone claiming to be John Smith. This process acknowledges that human morality is weak and that machines are needed to preserve the users privacy. A machine can be prescribed to maintain morality better that any human according to Latour (1993). This is also reflected in both Interviewee 3 and 4 statements that clever social engineers can persuade Vodafone call centre personnel into giving out information even though they fail standard questions designed to eliminate fraudsters. This may enable callers to get John Smiths information by persuading call centre employees that they are indeed John Smith but have forgotten the password. A complete elimination of this problem is impossible, it would require a surveillance of every call centre employee. The surveillance apparatus would soon become as large in size as the call centre itself. It would also raise the age-old question on who will inspect the inspectors.

The example of John Smith shows that some humans have what Latour would call an antiprogram to the designer's program (1992, p. 247). The intention of the designer is that privacy should be maintained. Computer hackers, disloyal employees and competitors that are willing to use unlawful and unwanted methods to gain access to SensorPhone data, contradicts the user's and Vodafone's wish for privacy. The solution to the antiprogram is to include technical, contractual and organisational measures in the program to keep the data safe (Interviewee 1,3,4). A technical authentication processes in the system enables the system to brace itself against the

unwanted use. By creating a nonhuman, technical guardian of morality Vodafone relieves the humans from the temptation to commit data theft.

When Vodafone start using encrypted data communication and demanding login passwords they inscribe that the data is private. To be enquired for a password when browsing the SensorPhone website communicates a division of people, those who are accepted and those who are not, users and non-users. Much in the same way a locked file-cabinet communicates that only key-holders are entitled to look at the files contained within, while a partially open cabinet invites anyone to snoop. The solution to low morality amongst humans is to create a nonhuman technological guardian of morality and values in the authentication function. An authentication function does not only prevent non-users from snooping, but also real users since a user will only be able to access personal data, not the other user's data. At the same time the responsibility for data is partially transferred from Vodafone to the user. The user is however required to keep their password a secret and not share it with others.

Unauthorised data access is not only a problem externally; Vodafone employees can be an equal or greater threat to customer privacy as external sources. Latour (1992) describe a situation where it is impossible to control employees behaviour according to company wishes. The threat is that employees can intentionally provide data to external sources. Some efforts are initiated by Vodafone to avoid customer data on the loose. One of these is to limit the number of humans that are allowed partial or full access to data.

Interviewee 3 explains that Vodafone uses both technical and organisational measures to maintain data security, such as logical access, access based on business needs and incident reporting, all aimed to limit access to data. In addition Vodafone tries to build a company culture that focuses on security and privacy. The Vodafone

security group holds lectures to all employees to educate them on the importance of proper security. A small portion of Vodafone employees are trusted computer administrators that must always be able to access the system to ensure it's operationally. In other words Vodafone trust that they are able to employ administrators with high morality. Interviewee 5 presents an opposing view when stating that anyone at Vodafone can access customer call details. This is intended as a customer service function, that anyone should be able to aid when the customer needs a new SIM-card or has questions regarding billing. While it is a good example of customer service, it is a bad example of privacy management. 2500 employees at Vodafone can view call details on all Vodafone customers in the Netherlands. This is how the example in chapter 3.3 regarding sale of phone records happened.

The connection between the patient and the doctor will also be maintained electronically, with machines that maintain a constant level of morality. The SensorPhone will only transmit data to another machine when a username and password identify the enquirer as a legitimate doctor to a specific patient. A computer hacker can of course challenge this, but that will require a highly specialised competence limiting the number of humans that are able to do this.

Here we see Vodafone employing technology to limit both internal and external access to data. The designer inscribes the technology with a minimum of moral standards within the system, regardless of the morality of the users. By transferring the responsibility of ethics to stubborn machines one archives a constant level of morality and a minimum acceptable level of privacy maintenance.

5.2. Changes During the Systems Life-Cycle

Some products never reach a stable state. Consider the most popular computer operating system today, Microsoft Windows XP. Since its launch it has had numerous

major and minor updates as responses to new development in technology, how the users actually use the operating system and flaws in the original product. The Internet makes it possible for Microsoft to gather error reports created by Windows XP and distribute updates to prevent future similar errors in an affordable and efficient way.

A similar system already exists in the mobile phone network. It is possible for Vodafone to upgrade the software on the phones of their subscribers without physically accessing the phones (Interviewee 3). The servers that store and process the SensorPhone data can naturally be accessed and upgraded by Vodafone when they wish. Upgrades can range from minor adjustment to major changes in the software. The dilemma this poses is that when upgrading the system, functionality can be altered, and how will the users interest be maintained in such a situation? Will the user always be aware of the update and what the update does?

One can imagine that it is desirable at some point to add the feedback provided by a real life nutrition exper, in addition to the advice from the physician. Functionality would be added, but some loss of privacy would be required. Based on the user's data a personalised menu could be offered. This would require that the nutrition expert review the user's data, the users may not agree that a party not bound by medical ethics should be able to access their data. One of the ISTAG groups concerns was that technology would govern humans instead of the opposite. Further the data that the system creates belongs to the user and should therefore be controlled by the user.

Updating software while it is being used may then require a new contract between user and producer. There should be a realistic option for the user to choose not to accept added functionality at one point without at the same time having to forgo future updates.

5.3. Inscribing Simplicity

As mentioned in the description of SensorPhone it should be possible to install the system on almost any mobile phone, even simple models with just basic functionality. The reason for this is that Vodafone recognises that obesity is a disease that discriminates. The main socio-economic groups that are affected by obesity can be described briefly as low education / low income groups (Werrij, 2006, p. 16). This group may not be able to afford or understand expensive and advanced mobile phones and may not need the functionality those provide. By using low-end phones Vodafone includes this group among their projected users. If Vodafone wishes to inscribe privacy awareness they need to find simple, easy to understand ways of communicating that there is privacy, within the system. One method of doing this would be to make the contract and instruction that the user receives as simple as possible, as mentioned by Interviewee 2. A pictogram used by web-browsers can serve as an example here. When entering a secure website most browsers show a padlock on the address- or status bar. Similar symbols could be used in SensorPhone to reassure the user that privacy is maintained. A constant reminder on the phone screen in the form of a padlock or transparency in the log-on process showing that passwords are exchanged could be symbols showing that the system is secure.

A system that is designed to be intuitive in its use could face problems if a part of it is burdened with complex symbols, technical language and thick instruction manuals. The inscription Vodafone makes when using a low-end phone should be followed throughout the system to create a consistent communication with the real user.

5.4. Reflexive Users and Mediators

In the building of the SensorPhone I can identify both reflexive users and mediators. These two groups will participate in how the system is built and developed. The reflexive users are found among the system builders, and they are building the technology for themselves, assuming that what they want from the technology is also what the future users would want (Lindsay, 2005, p. 34).

My first sighting of the reflexive user in the SensorPhone was when one of the interviewees patted his stomach and stated that he certainly could use more exercise in his daily life. Two other interviewees also mentioned that the SensorPhone could be an aid for them to exercise more. Not that my interviewees suffered from obesity in any way, it was rather an acknowledgement that working long hours in offices contradicted a wish for a healthy lifestyle and that motivational features in SensorPhone could help change that.

The relation to privacy in this case is that several of the interviewees have a professional interest in privacy, mainly Interviewees 3 and 4. Interviewee 3 does not believe that privacy is a major issue for the average user of their telecommunication services. One claim is that if the service is beneficial then the user will subscribe without significant privacy concerns. On the other hand Interviewee 3 does claim to see how much goes wrong and can go wrong in a telecommunications company, something that the average customer is not aware of. Interviewee 3 would therefore build a system that maintains privacy, due to extensive knowledge on what can go wrong. For Interviewee 3 an elaborate security system would have to be in place to personally use a system.

Interviewee 4 is concerned that outside organisations will get hold of her personal data without explicit consent and that the resulting consequences will be

unwanted. Therefore, Interviewee 4 would ensure that the privacy of the user is maintained. Interviewee 4 also mentions that privacy laws do not give black and white answers to privacy issues. There are many grey areas and there is definitely room for interpretations. This empowers a law-abiding designer to decide behaviour based on personal wishes to a larger degree when inscribing values into their objects.

What we see here is that people within Vodafone have a personal wish to use a SensorPhone system and that for them to do so, certain criteria has to be in place. This will affect the final user, since they will benefit from the wishes of the reflected users within Vodafone.

The mediators are somewhat in between the builders and the users of the system even though they are also users (Lindsay, 2005, p. 37). One group planned to be important mediators in the SensorPhone are the physicians. If the physician's are supposed to be part of the system they will have some say in who the real user will be. It might be more specific in this case to talk about the wearer, since the doctor uses the data and is then also a user of the system. The doctor decides which patients will wear SensorPhone as a treatment device based on interpretations of how SensorPhone criteria match the patients' case thus creating users. The physicians can also be very influential in how the system will develop further. They can aid the decisions regarding which diagnostics and treatment are suitable to be taken out of the hospital and into the private home.

In the privacy aspect the physician has a responsibility to maintain the Hippocratic oath, therefore it is unlikely that the medical world will participate in a system that does not supply adequate privacy protection. A proper privacy practice will also be required to integrate SensorPhone into a national or trans-national electronic health record. If the physicians are not willing to participate in

SensorPhone it seriously limits it functionality as a medical system. Lack of support from the medical world would in practice mean that the projected user would be in the fitness segment only.

Another group that fitting Lindsay's mediator description are the insurance companies. I have earlier described this group as a group that might benefit from accessing the data in the system. The insurer might view the SensorPhone as a tool for ensuring that their users follow a treatment or as a method for calculating the insurance premium. My reason for including them as mediators is that they are likely to be the purchasers of the SensorPhone, just as they today pay for medicine for their clients. With national healthcare facing budgetary restraints and the population not always able to directly pay for medical treatment, the task is often left to the insurer. If the insurer is the one paying for the system, they will most certainly demand full or partial access to data and progress reports and can demand some saying in the development of the system. This contradicts the physicians' wish for patient – doctor confidentiality. However, medical and life insurers already require some insight into the client's medical record before agreeing to insure the person.

5.5. Privacy in a Business Context

Vodafone is a private business with the same aim as most other businesses, to maximise return on investments. Since Vodafone obtains large amount of information on their customers and they could easily sell this data for short-term profit it is relevant to discuss reasons against this. Interviewee 4 assured me that Vodafone Netherlands had never sold customer data and they had strict policies against just that, one should ensure that this practice continues.

Interviewee 3 claims that Vodafone management require the cost of increased security investments in their systems to be passed onto their customers. This shows

that management is an important entity that sets requirements for the products. *A secure product* can contradict *an affordable product* and it will be the management's responsibility to ensure that the optimal mix between *security* and *affordability* is achieved.

We can for a moment look at a marketing concept corporate social responsibility (CSR). CSR dictates that the general public view companies as morally responsible for their actions other than purely financial, and that this view determines whether or not they will become a customer. While I have not been able to tie any case studies to privacy directly, my claim is that privacy is a part of CSR. Bhattacharya and Sen's (2004, p. 23) research on CSR and consumers response to CSR initiative concludes that consumers are more sensitive to negative CSR information than positive. The implication is that a discovery of bad or sloppy privacy management from Vodafone's side will have a greater negative impact on their reputation than proper privacy management would have as a positive impact. In an industry where the costumers can change suppliers as easily as in the telecommunication industry it becomes important for suppliers to maintain a good reputation.

One of the great barriers to proper CSR is the short-term investment usually associated with western culture. The return on investments from CSR efforts is usually long-term and competes with other investments with a short-term yield. Most western companies will chase quarterly profits and avoid long-term investments due to the number of uncertainties involved (White, 2006).

Vodafone is here no different from other industrial actors according to Interviewee 5. Interviewee 5 complains that company culture dictates that short-term market opportunities such as the soccer world cup and the UMTS technical solutions

overshadow the potential of a long-term investment in the grey market[13] and health solutions. As with CSR, these are markets that require time to build.

This shows that Vodafone management have two contradicting issues. On one side they have a wish to create revenue by increasing income and cutting costs. On the other side they need to preserve the privacy and security of their customers and their own reputation. Interviewee 3 states that all cost related to security is passed on to the consumer, thus becoming a part of the market package. Managerial decisions on the level of price and security will therefore affect Vodafone's new products and how it is received in the market.

Proper privacy management is not a focus area in the consumers mind at the present time. However, as I stated in the previous chapters, this can easily change and strong privacy protection can in the long term become a strong selling point in the consumer market. My point here is that the culture for short-term profit found in Vodafone should not exploit the potential revenue in personal data. Privacy management should instead be viewed as a long-term investment, not just a cost forced upon the company by regulators.

5.6. Conclusion

As the SensorPhone is being developed at this time it is most difficult to describe all the forces that affect the system. However, I have in this chapter outlined some factors that most likely will be a part of it. When the designer has a wish to build privacy maintaining elements into the system they simultaneously transfer the responsibility for keeping morality from humans but into objects. The morality can be maintained by e.g. an authentication process to be able to view data, and the effect on the user will be different depending on how this process is presented. The

authentication would be a program for how the system braces itself against what the designers regard as unwanted behaviour, the real users antiprogram.

Internal measures for lowering the risk for internal data theft or spillage are also put in place by Vodafone. Both technical and organisational efforts are used. However, Vodafone acknowledges that it is impossible to completely remove the risk that an employee, either on purpose or by accident, is the source for security breaches.

I have also argued that there are reflexive users within Vodafone that will affect the SensorPhone system with regards to privacy. Sources claim that their average customers are not interested in privacy and that they see it as their responsibility then that Vodafone's privacy policies are stronger than both the customers would care for and the law requires. However the designer cannot just rely on their own view of the end-user, or their own wishes as users, the demands of other entities will affect the final product. Further mediators that are planned to be a part of the SensorPhone, such as physicians and insurers have their own agenda when it comes to the data in the system. The challenge of finding a privacy practice that the different groups can accept will ultimately be a task for Vodafone management.

---

[13] The grey market here refers to a market segment, not a sales on the borderline to the illegal black market. The grey segment is named after the colour of hair and can be described as 50+ years, in good health, on the top of their carriers, with house mortgages paid down and grown, out of the nest, children. This is a segment with money.

6. Summary

In this thesis I have summarised the discussion surrounding ambient intelligence and privacy. Strong forces claim that privacy belongs in history, while others believe that it is more important now than ever before. One of the most interesting discoveries that I made during my work on this thesis is that the discussion now is almost identical to the one started by Warren and Brandeis in 1890. Their claim was that technology, if not treated in a morally acceptable way, can be a threat to people's privacy. The real question that will not be answered until the technology arrives is whether or not the public themselves will refuse to use AmI with a weak privacy protection or if the benefits from the technology will outweigh concerns.

In the case of SensorPhone my claim is still that it faces many of the privacy issues that ambient intelligence is faced with. Important issues for Vodafone here will be; who should get access to the users data and how can the user remain in charge of data. An important function for the SensorPhone is sharing of data, a result of that is loss of privacy to some extent. This may be acceptable if the sharing of data is necessary to create a superior service for the user. Finally, and maybe in the future most importantly, is how should Vodafone and the devices in SensorPhone communicate to the user that privacy is maintained without overloading the user with information.

What should be clear is that the end-user is not the only actor with concerns regarding privacy. Privacy will be the result of mediation between the designers, the real users and the different actors with different interests in the data. Further it is a matter of cost and the consumer's willingness to pay for security versus functionality.

6.1. Implications and Recommendations

As I previously mentioned in chapter four, it will be most important to assess how the real user view's the privacy aspect. How much the different entities within the system are trusted will determine the user's willingness to share data. While not all the users who wear the system will consider privacy as a factor, the physicians that receive the data will have to maintain the Hippocratic oath, and part of that includes securing the privacy of the patients. Therefore, it is in my opinion vital that strong privacy protection is inscribed in the system. A positive side effect of this will be that theft or leakage of data will be less plausible. Programs for maintaining privacy should be initiated at the earliest stage so that the first product generation have proper protection, this will ensure that privacy is inscribed into latter generations as well.

The dilemma that potential users, Vodafone management, doctors and insurers have differing views on privacy is a conflict that has to be addressed. All entities are needed in the system, so each group has to be considered when designing the business model. To make a complete list of which entities must be included for SensorPhone to become a successful medical device is unfortunately beyond the scope of this thesis. But my recommendation is that such a survey is preformed. According to Interviewee 5 there is a myriad of actors all of them are vital to please if the system is to be successful.

6.2. Future Research

It is my belief that the SensorPhone can be used as a case for almost an endless range of STS topics. These include governmental policy making for new methods of treatment. Also cyborg theories can be investigated from a SensorPhone perspective, where science is used to monitor the body, not only for enhancement or replacement.

A review after the system has been operational for some time would provide useful information on whether or not privacy is an issue for the users.

Vodafone should initiate or join current research efforts into making a secure seal for use on products that gather and process personal information. Such a seal might prove to be beneficial if the general public start to view their personal data as something that should be protected.

7. References

7.1. Date of Interviews

I have chosen to withhold the names of my interviewees so that they could speak more freely. To be able to use the interviews as an academic source all interviews were recorded and the materials are in my personal archive. All interviews were conducted at Vodafone offices in Maastricht, Netherlands.

Interviewee 1 conducted April 24th 2006

Interviewee 2 conducted June 15th 2006

Interviewee 3 conducted July 11th 2006

Interviewee 4 conducted July 11th 2006

Interviewee 5 conducted July 27th 2006

7.2. Bibliography

Adams, A., & Sasse, M. A. (2001). *Privacy in Multimedia Communications: Protecting Users, Not Just Data.* Paper presented at the People and Computers XV - Interactions without frontiers, Lille.

Akrich, M. (1992). The de-scription of technical objects. In W. E. Bijker & J. Law (Eds.), *Shaping technology/building society: Studies in sociotechnical change* (pp. 205-224). Cambridge, MA: MIT Press.

Blarkom, G. W. v., Borking, J. J., & Olk, J. G. E. (Eds.). (2003*). Handbook of Privacy and Privacy-Enhancing Technologies - The case of intelligent software Agents*. The Hague: TNO-FEL.

Brey, P. (2005). Freedom and Privacy in Ambient Intelligence. *Ethics and Information Technology*, 7(3), 157 - 166.

British Information Commissioner's Office. (2005). *Annual Track – Individuals*. Kingston upon Hull. Retrived May 20, 2006, from www.smsr.co.uk

Casert, R. (2004, November 8, 2004). *Rathenau Institute's Workshop Ambient Intelligence: In the service of man*. Paper presented at the EUSAI2004 symposium, Eindhoven University of Technology, the Netherlands.

Celler, B. G., Lovell, N. H., & Chan, D. K. Y. (1999). The Potential Impact of Home Telecare on Clinical Practices. *The Medical Journal of Australia*, 171(10), 518-521.

Clemet, K. (2006, June 23. - 29. 2006). Privatlivets Fred. *Morgenbladet*, p. 40.

Doney, P. M., & Cannon, J. P. (1997). An Examination of the Nature of Trust in Buyer - Seller Ralationships. *Journal of Marketing, 61*(2), 35-51.

Ducatel, K., Bogdanowicz, M., Scapolo, F., Leijten, J., & Burgelman, J.-C. (2001). Scenarios for Ambient Intelligence. Seville: ISTAG.

Emiliani, P. L., & Stephanidis, C. (2005). Universal access to ambient intelligence environments: Opportunities and challenges for people with disabilities. *IBM Systems Journal, 44*(3).

European Commission. (2003). Data Protection – Highlights. Special Eurobarometer 196 – Wave 60.0 – European Opinion Research Group EEIG.

Ford, R. (2004, August 16th, 2004). Beware rise of Big Brother state, warns data watchdog. *The Times*.

Friedewald, M., Vildjiounaite, E., & Wright, D. (eds.) "The brave new world of ambient intelligence. Deliverable D1. A report of the SWAMI consortium to the European Commission under contract 006507. June 2005. Retrieved March 28, 2006, from: http://swami.jrc.es"

Gripsrud, G., & Olsson, U. H. (2000). *Markedsanalyse*. Kristiansand S: Norwegian Academic Press.

Grigsby, J., & Sanders, J. H. (1998). Telemedicine: Where It Is and Where It's Going. *Ann Intern Med*, 129(2), 123-127.

Hu, X., Lin, Z., & Zhang, H. (2003). Myth or Reality: Effect of Trust-Promoting Seals in Electronic market. In O. Petrovic, R. Posch & F. Marhold (Eds.), *Trust in Network Economy* (pp. 143-150). Wien: Springer.

Krim, J. (2005, July 8, 2005). *Online data gets personal: cell phone records for sale*. Retrieved August 7, 2006, from: http://www.washingtonpost.com/wp-dyn/content/article/2005/07/07/AR2005070701862_pf.html

Langheinrich, M. (2001). *Privacy by design - Principles of Privacy-Aware Ubiquitous Systems*. Paper presented at the Ubicomp 2001: Ubiquitous Computing: Third International Conference, Atlanta, Georgia, USA.

Latour, B. (1992). Where are the Missing Masses? Sociology of a Few Mundane Artifacts. In W. E. Bijker & J. Law (Eds.), *Shaping Technology/Building Society: Studies in Sociotechnical Change* (pp. 205-224). Cambridge, MA: MIT Press.

Lindsay, C. (2005). From the Shadows: Users as Designers, Producers, Marketers, Distributors, and Technical Support. In N. Oudshoorn & T. Pinch (Eds.), *How Users Matter: The Co-Construction of Users and Technology* (pp. 29-50). London: MIT Press.

Maranta, A., Guggenheim, M., Gisler, P., & Pohl, C. (2003). The Reality of Experts and the Imagined Lay Person. *Acta Sociologica, 46*(2), 150-165.

NICTIZ. (2006, 20th and 21th March 2006). *Summary and Conclutions.* Paper presented at the Health ID Managment Workshop, Amsterdam.

Norwegian Data Advicory Board. (2006). Personvernrapporten 2006: Retten til å være i fred. Oslo: Datatilsynet. Retrived June 12, 2006, from: http://www.datatilsynet.no/templates/Page____1428.aspx

Oudshoorn, N., & Pinch, T. (2005). How Users and Non-Users Matter. In N. Oudshoorn & T. Pinch (Eds.), *How Users Matter: The Co-Construction of Users and Technology* (pp. 1-28). London: MIT Press.

Potter, N. (2005, Feb 6, 2006). *Why are your cell phone records for sale?*. Retrieved August 7, 2005, from: http://abcnews.go.com/WNT/Business/story?id=1585840

Poston, W. S. C., & Foreyt, J. P. (2000). Successful Managment of the Obese Patient. *American Academy of Family Physicians, 61*(12).

Punie, Y., Delaitre, S., Maghiros, I. & Wright, D. (eds.) (2005). "Dark scenarios on ambient intelligence: Highlighting risks and vulnerabilities". SWAMI Deliverable D2. A report of the SWAMI consortium to the European Commission under contract 006507, November 2005. Retrieved March 28, 2006, from: http://swami.jrc.es

Reuters. (2006). *Heads Roll in AOL Affair*. Retrieved August 13th, 2006, from: http://www.wired.com/news/technology/0,71628-0.html?tw=rss.index

Riegelsberger, J., & Sasse, M. A. (2001). Trustbuilders and Trustbusters In *Proceedings of the IFIP Conference on Towards The E-Society: E-Commerce, E-Business, E-Government* (pp. 17-30): Kluwer, B.V.

Riel, C. B. M. v. (1992). *Principles of Corporate Communication*. Essex: Prentice Hall.

Soede, M. (2005, October 7, 2005). Ambient Intelligence and Disability: Where do they meet? Abstract and presentation at the COST 219ter Cyprus Workshop, Aya Napa.

Tulloch, J., & Lupton, D. (2003). *Risk and Everyday Life*. London: SAGE Publications.

Verbeek, P. P. (2006). Materializing Morality - Design Ethics and Technology Mediation. *Science, Technologies and Human Values, 31*(3), 361-380.

Vodafone (2005). Annex B, Project plan – Mobile telephone based wireless patient activity monitoring and telecare system using wearable 3-D motion sensors (SensorPhone). (Personal archive)

Vodafone (2006), "CeBIT 2006 – Vodafone Biozoom." (Personal archive)

Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. Harvard Law Review, 4(5).

Werrij, M. (2005). *Weighty Thoughts. A cognitive approach to the treatment of obesity*. Maastricht: Maastricht University.

Westin, A. (1967). *Privacy and Freedom*. New York: Atheneum.

White, A. (2006). *The Grasshoppers and the Ants: Why CSR Needs Patient Capital*. Retrieved August 29th, 2006, from http://www.bsr.org/meta/200605_Patient-Capital.pdf

World Medical Association. (1948) "*Declaration of Geneva – The Hippocratich Oath*." Retrieved July 19, 2006, from: http://www.wma.net/e/policy/c8.htm

7.3. List of Abbreviations

AmI – Ambient Intelligence

ANT – Actor Network Theory

AOL – American Online

BICO - The British Information Commissioners Office

CEO – Chief Executive Officer

CSR – Corporate Social Responsibility

DAA - data acquisition and analysis device, a component of the SensorPhone

EU – European Union

iRv - The Institute for Rehabilitation Research / Kenniscentrum voor Revalidatie en Handicap

ISO – International Organization for Standardization

ISTAG - Information Society Technology Advisory Group

NATO – North Atlantic Treaty Organization

NDPA - The Norwegian Data Protection Agency (*Datatilsynet*)

NICTIZ – National IT institute for healthcare in the Netherlands

PIM – Personal Information Manager

R&D – Research and Development

UMTS - Universal Mobile Telecommunications System

STS – Science and Technology Studies

8. Appendix A: Ambient Intelligence Scenarios

This is a small description on the positive scenarios in Scenarios for Ambient Intelligence in 2010, the whole description with scenarios and analysis can be downloaded at www.cordus.lu/ist/istag.htm

1) The individual – efficient scenario pictures road-warrior Maria who travels to unknown country, AmI unlocks doors, direct her to her car, blocks incoming phone calls when she is stressed, customises presentation to fit local taste.
2) In the individual – social humanistic scenario we see Dimitios and his D-Me (digital me device) that handle calls and requests so that Dimitios will not be disturbed unnecessarily. The device interprets how important the call is and if less important it can conduct small conversations. It takes care of a request for information from another D-Me without disclosing information about Dimitios.
3) The community – efficiency scenario describes Carmen and her AmI device that finds someone with a similar travel plan as her and arranges a shared ride, and arranges payment. Due to congestion the AmI suggest alternative routes involving the metro. She grocery shops and arranges delivery on AmI. Finally the AmI suggest telework due to planned demonstration downtown the next day.
4) This last community – social humanistic scenario describes AmI in the in a social learning environment. A meeting in an environmental studies group. AmI schedules participants and creates workgroups based on knowledge and interests. AmI directs the attention to a mentor to where it is most needed.

The negative scenarios are presented in deliverable two in the Safeguards in a World of Ambient Intelligence papers (Punie et. al. 2005). These scenarios highlight some of

the dangers in ambient intelligence and the object of the paper is to promote a discussion on these topics. For the full scenarios with analysis see: www.cordus.lu/ist/istag.htm

1) The first scenario deals with the individual – efficiency questions and describes situations where privacy and security efforts are not sufficient at home, at work and in public. Inadequate profiling result in a police investigation. A Personal message is broadcasted in public and creates embarrassing scene. Loss of control, spy-ware and personalised spam becomes limits the use of AmI.
2) The community – social humanistic dark scenario describes a group of seniors on a bus journey. Decisions are left up to computerised systems with the result that simple errors result in denial of service. Persons using software they are not entitled to caused a traffic accident. AmI devices prioritise medical treatment depending on how injured the victims are, but also on their insurance. Lack of compatibility between AmI systems and to much dependability in technology results in a fatality.
3) In scenario three, the community – efficiency scenario, a data collecting company is followed in a boardroom meeting and a court case. The company exploits loopholes in legislation and differences between national laws to create extensive profiles on citizens. Profiling is used to identify people considered to be a security risk or that exhibits anti-social behaviour. Implants and electronic trails are used to track the location of employees. The profiles in the scenario can be inaccurate and the responsibility for accuracy is unclear.

4) The forth, community - social humanistic scenario is the most distant scenario in time. We follow the morning TV broadcast and an interview with the Anti-personalised-profiling action group. The interviewee describes a how AmI devices and surrender of privacy, is a requirement to participate in most events. The interviewee further describes that profiling threatens free choice. A situation where a computer virus shuts down a city's road management system, creating chaos in the inner city is described. The last fictional news story is a public concert where those without AmI devises are not notified when a stadium needs to be evacuated.